ZyAIR B-2000

Wireless LAN Gateway with 4-Port Switch

User's Guide

Version 3.50

October 2002

ZyXEL

TOTAL INTERNET ACCESS SOLUTION

Copyright

Copyright © 2002 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Certifications

Refer to the product page at www.zyxel.com.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Safety Warnings

1. To reduce the risk of fire, use only No. 26 AWG or larger telephone wire.

2. Do not use this product near water, for example, in a wet basement or near a swimming pool.

3. Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightening.

Customer Support

Please have the following information ready when you contact customer support.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD LOCATION	E-MAIL SUPPORT/SALES	TELEPHONE/FAX	WEB SITE/ FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu 300, Taiwan.
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-714-632-0882 800-255-4101 +1-714-632-0858	www.zyxel.com ftp.zyxel.com	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
SCANDINAVIA	support@zyxel.dk sales@zyxel.dk	+45-3955-0700 +45-3955-0707	www.zyxel.dk ftp.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark.
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A4 D-52146 Wuerselen, Germany

Table of Contents

Copyright ..... **ii**
Federal Communications Commission (FCC) Interference Statement ..... **iii**
ZyXEL Limited Warranty ..... **iv**
Customer Support ..... **v**
List of Figures ..... **xi**
List of Tables ..... **xv**
List of Diagrams ..... **xvi**
Preface ..... **xvii**
GETTING STARTED ..... **I**
Chapter 1 Getting To Know Your ZyAIR **1-1**
1.1 ZyAIR B-2000 Wireless LAN Gateway with 4-Port Switch 1-1
1.2 Features of the ZyAIR 1-1
1.3 Application for the ZyAIR 1-4
1.3.1 Broadband Internet Access via Cable or DSL modem 1-4
Chapter 2 Hardware Installation and Initial Setup **2-1**
2.1 Front Panel LEDs of the ZyAIR 2-1
2.2 Side Panel and Connections of the ZyAIR 2-3
2.2.1 WAN Port 2-3
2.2.2 Four LAN 10/100M Ports 2-3
2.2.3 Console Port 2-4
2.2.4 Restore Factory Defaults/Reset Button 2-4
2.2.5 Power Port 2-4
2.2.6 F.G. (Frame Ground) 2-4
2.2.7 Antennas 2-4
2.3 Hardware Mounting Options 2-5
2.4 Additional Installation Requirements 2-5
2.5 ZyAIR Configuration 2-6
2.5.1 Connect to Your ZyAIR Using the Web Configurator 2-6
2.5.2 Connect to your ZyAIR Using Telnet 2-6
2.5.3 Connect to Your ZyAIR Using the Console Port 2-6
2.5.4 Initial Screen 2-7
2.5.5 Entering Password 2-7
2.6 Resetting the ZyAIR 2-8
2.6.1 Methods of Restoring Factory-Defaults 2-8
2.6.2 ZyAIR SMT Menu Overview 2-8
2.7 Navigating the SMT Interface 2-10
2.7.1 System Management Terminal Interface Summary 2-11
2.8 Changing the System Password 2-12
2.9 General Setup 2-12

2.9.1 Dynamic DNS 2-13
2.9.2 Procedure To Configure Menu 1 2-13
2.9.3 Procedure to Configure Dynamic DNS 2-14
2.10 WAN Setup 2-15
2.11 LAN Setup 2-16
2.11.1 General Ethernet Port Filter Setup 2-17
Chapter 3 Internet Access 3-1
3.1 Factory Ethernet Defaults 3-1
3.2 LANs and WANs 3-1
3.2.1 LANs, WANs and the ZyAIR 3-1
3.3 TCP/IP Parameters 3-2
3.3.1 IP Address and Subnet Mask 3-2
3.3.2 Private IP Addresses 3-3
3.3.3 RIP Setup 3-3
3.3.4 DHCP Configuration 3-4
3.4 IP Multicast 3-5
3.5 TCP/IP Ethernet and DHCP Setup 3-5
3.6 IP Alias 3-7
3.6.1 IP Alias Setup 3-8
3.7 Encapsulation 3-10
3.7.1 Ethernet 3-10
3.7.2 PPPoE 3-10
3.7.3 PPTP 3-10
3.8 IP Address Assignment 3-11
3.9 Internet Access Configuration 3-11
3.10 Internet Access Setup 3-12
3.11 Wireless LAN 3-13
3.11.1 Wireless LAN Parameters 3-13
3.11.2 Wireless LAN Setup 3-15
3.11.3 Roaming 3-16
3.11.4 Requirements for Roaming 3-17
3.11.5 Enable the Roaming Feature on the ZyAIR 3-18
ADVANCED APPLICATIONS II
Chapter 4 Wireless LAN Security Setup 4-1
4.1 Levels of Security 4-1
4.2 Data Encryption with WEP 4-1
4.3 Network Authentication 4-3
4.3.1 EAP 4-3
4.3.2 RADIUS 4-3
4.3.3 Sequence for EAP Authentication 4-4
4.3.4 Enable EAP Authentication on Your ZyAIR 4-5

4.3.5 Configuring External RADIUS Server 4-6
4.4 Creating User Accounts on the ZyAIR 4-7
4.5 MAC Address Filtering 4-8
Chapter 5 Remote Node Configuration 5-1
5.1 Remote Node Profile 5-1
5.1.1 Encapsulation Scenarios 5-1
5.1.2 Outgoing Authentication Protocol 5-4
5.1.3 Remote Node Setup 5-4
5.2 Remote Node Filter 5-6
5.2.1 IP Static Route Setup 5-7
Chapter 6 Network Address Translation (NAT) 6-1
6.1 Introduction 6-1
6.1.1 NAT Definitions 6-1
6.1.2 What NAT Does 6-2
6.1.3 How NAT Works 6-2
6.1.4 NAT Application 6-3
6.1.5 NAT Mapping Types 6-4
6.2 Using NAT 6-6
6.2.1 SUA (Single User Account) Versus NAT 6-6
6.2.2 Applying NAT 6-6
6.3 NAT Setup 6-7
6.3.1 Address Mapping Sets 6-8
6.3.2 Configuring Individual Rule 6-11
6.4 NAT Server Sets – Port Forwarding 6-12
6.4.1 Configuring a Server behind NAT 6-13
6.5 General NAT Examples 6-16
6.5.1 Example 1: Internet Access Only 6-16
6.5.2 Example 2: Internet Access with an Inside Server 6-17
6.5.3 Example 3: Multiple Public IP Addresses With Inside Servers 6-18
6.5.4 Example 4: NAT Unfriendly Application Programs 6-21
ADVANCED MANAGEMENT III
Chapter 7 Filter Configuration 7-1
7.1 About Filtering 7-1
7.2 Configuring a Filter Set 7-3
7.2.1 Filter Rules Summary Menus 7-5
7.3 Configuring a Filter Rule 7-6
7.3.1 TCP/IP Filter Rule 7-6
7.3.2 Generic Filter Rule 7-11
7.4 Filter Types and NAT 7-12
7.5 Example Filter 7-13
7.6 Applying Filters and Factory Defaults 7-15

7.6.1 Ethernet Traffic 7-16
7.6.2 Remote Node Filters 7-16
Chapter 8 SNMP Configuration 8-1
8.1 About SNMP 8-1
8.2 Supported MIBs 8-2
8.3 SNMP Configuration 8-2
8.4 SNMP Traps 8-3
Chapter 9 System Information and Diagnosis 9-1
9.1 System Status 9-1
9.2 System Information 9-3
9.2.1 System Information 9-3
9.2.2 Console Port Speed 9-4
9.3 Log and Trace 9-4
9.3.1 Viewing Error Log 9-5
9.3.2 UNIX Syslog 9-5
9.3.3 Call-Triggering Packet 9-7
9.4 Diagnostic 9-7
Chapter 10 Firmware and Configuration File Maintenance 10-1
10.1 Filename Conventions 10-1
10.2 Backup Configuration 10-2
10.2.1 Backup Configuration 10-3
10.2.2 Using the FTP Command from the Command Line 10-3
10.2.3 Example of FTP Commands from the Command Line 10-4
10.2.4 GUI-based FTP Clients 10-4
10.2.5 TFTP and FTP over WAN Will Not Work When 10-4
10.2.6 Backup Configuration Using TFTP 10-5
10.2.7 TFTP Command Example 10-5
10.2.8 GUI-based TFTP Clients 10-5
10.2.9 Backup Via Console Port 10-6
10.3 Restore Configuration 10-7
10.3.1 Restore Using FTP 10-8
10.3.2 Restore Using FTP Session Example 10-9
10.3.3 Restore Via Console Port 10-9
10.4 Uploading Firmware and Configuration Files 10-10
10.4.1 Firmware File Upload 10-10
10.4.2 Configuration File Upload 10-11
10.4.3 FTP File Upload Command from the DOS Prompt Example 10-12
10.4.4 FTP Session Example of Firmware File Upload 10-12
10.4.5 TFTP File Upload 10-12
10.4.6 TFTP Upload Command Example 10-13
10.4.7 Uploading Via Console Port 10-13

10.4.8 Uploading Firmware File Via Console Port 10-14
10.4.9 Example Xmodem Firmware Upload Using HyperTerminal 10-14
10.4.10 Uploading Configuration File Via Console Port 10-15
10.4.11 Example Xmodem Configuration Upload Using HyperTerminal 10-15
Chapter 11 System Maintenance and Information 11-1
11.1 Command Interpreter Mode 11-1
11.2 Time and Date Setting 11-2
11.2.1 Resetting the Time 11-3
Chapter 12 Call Scheduling 12-1
12.1 Introduction 12-1
Chapter 13 Remote Management 13-1
13.1 Telnet 13-1
13.2 FTP 13-1
13.3 Web 13-1
13.4 Remote Management 13-1
13.4.1 Remote Management Setup 13-2
13.4.2 Remote Management Limitations 13-3
13.5 Remote Management and NAT 13-3
13.6 System Timeout 13-4
ADDITIONAL INFORMATION IV
Chapter 14 Troubleshooting 14-1
14.1 Problem Starting Up the ZyAIR 14-1
14.2 Problem with the Password 14-1
14.3 Problem with the Ethernet Interface 14-2
14.4 Problem with the WAN Interface 14-2
14.5 Problem with Internet Access 14-3
14.6 Problem with Telnet 14-3
Appendix A Wireless LAN and IEEE 802.11 ..... A
Appendix B Wireless LAN With IEEE802.1x ..... E
Appendix C Antenna Selection and Positioning Recommendation ..... G
Appendix D PPPoE I
Appendix E PPTP ..... K
Appendix F TCP/IP ..... O
Appendix G IP Subnetting ..... U
Appendix H Power Adapter Specifications CC
Index ..... EE

List of Figures

Figure 1-1 Internet Access Application 1-4
Figure 2-1 ZyAIR Front Panel 2-1
Figure 2-2 ZyAIR Side Panel and Connections 2-3
Figure 2-3 Power-On Display 2-7
Figure 2-4 Login Screen 2-7
Figure 2-5 ZyAIR SMT Menu Overview 2-9
Figure 2-6 SMT Main Menu 2-11
Figure 2-7 Menu 23 – System Password 2-12
Figure 2-8 Menu 1 – General Setup 2-13
Figure 2-9 Configure Dynamic DNS 2-14
Figure 2-10 Menu 2 – WAN Setup 2-16
Figure 2-11 Menu 3 – LAN Setup 2-17
Figure 2-12 Menu 3.1 – General Ethernet Setup 2-17
Figure 3-1 LAN & WAN IPs 3-2
Figure 3-2 Menu 3.2 – TCP/IP and DHCP Ethernet Setup 3-6
Figure 3-3 Physical Network 3-8
Figure 3-4 Partitioned Logical Networks 3-8
Figure 3-5 Menu 3.2-TCP/IP and DHCP Setup 3-8
Figure 3-6 Menu 3.2.1-IP Alias Setup 3-9
Figure 3-7 Internet Access Setup 3-12
Figure 3-8 RTS Threshold 3-14
Figure 3-9 Menu 3.5 - Wireless LAN Setup 3-15
Figure 3-10 Roaming Example 3-17
Figure 3-11 Wireless LAN Setup 3-18
Figure 3-12 Menu 3.5.2 – Roaming Configuration 3-18
Figure 4-1 ZyAIR Wireless Security Levels 4-1
Figure 4-2 Wireless LAN Setup 4-2
Figure 4-3 Sequence for EAP Authentication 4-4
Figure 4-4 Menu 23 – System Security 4-5
Figure 4-5 Menu 23.4- System Security – IEEE802.1X 4-5
Figure 4-6 Menu 23.2 System Security - External Server 4-6
Figure 4-7 Menu 14- Dial-in User Setup 4-8
Figure 4-8 Menu 14.1- Edit Dial-in User 4-8
Figure 4-9 Menu 3.5 – Wireless LAN Setup 4-9
Figure 4-10 Menu 3.5.1 – WLAN MAC Address Filter 4-9
Figure 5-1 Menu 11.1 - Remote Node Profile 5-2
Figure 5-2 Remote Node Network Layer Options 5-5
Figure 5-3 Menu 11.5 - Remote Node Filter (Ethernet Encapsulation) 5-7
Figure 5-4 Menu 11.5 - Remote Node Filter (PPTP or PPPoE Encapsulation) 5-7

Figure 5-5 Sample Static Routing Topology 5-8
Figure 5-6 Menu 12.1 - IP Static Route Setup 5-8
Figure 5-7 Edit IP Static Route 5-9
Figure 6-1 How NAT Works 6-3
Figure 6-2 NAT Application With IP Alias 6-4
Figure 6-3 Menu 4 - Applying NAT for Internet Access 6-6
Figure 6-4 Menu 11.3 - Applying NAT to the Remote Node 6-7
Figure 6-5 Menu 15 - NAT Setup 6-8
Figure 6-6 Menu 15.1 - Address Mapping Sets 6-8
Figure 6-7 Menu 15.1.255 - SUA Address Mapping Rules 6-9
Figure 6-8 Menu 15.1.1 - First Set 6-10
Figure 6-9 Menu 15.1.1.1 - Editing/Configuring an Individual Rule in a Set 6-11
Figure 6-10 Menu 15.2 - NAT Server Setup 6-14
Figure 6-11 Multiple Servers Behind NAT Example 6-15
Figure 6-12 NAT Example 1 6-16
Figure 6-13 Menu 4 - Internet Access & NAT Example 6-16
Figure 6-14 NAT Example 2 6-17
Figure 6-15 Menu 15.2.1 - Specifying an Inside Server 6-17
Figure 6-16 NAT Example 3 6-18
Figure 6-17 Example 3: Menu 11.3 6-19
Figure 6-18 Example 3: Menu 15.1.1.1 6-19
Figure 6-19 Example 3: Final Menu 15.1.1 6-20
Figure 6-20 NAT Example 4 6-21
Figure 6-21 Example 4: Menu 15.1.1.1 6-21
Figure 6-22 Example 4: Menu 15.1.1 6-22
Figure 7-1 Outgoing Packet Filtering Process 7-1
Figure 7-2 Filter Rule Process 7-2
Figure 7-3 Menu 21 – Filter Set Configuration 7-3
Figure 7-4 NetBIOS_WAN Filter Rules Summary 7-4
Figure 7-5 NetBIOS_LAN Filter Rules Summary 7-4
Figure 7-6 TEL_FTP_WEB_WAN Filter Rules Summary 7-4
Figure 7-7 Menu 21.1.1 – TCP/IP Filter Rule 7-7
Figure 7-8 Executing an IP Filter 7-10
Figure 7-9 Menu 21.4.1 – Generic Filter Rule 7-11
Figure 7-10 Protocol and Device Filter Sets 7-13
Figure 7-11 Sample Telnet Filter 7-13
Figure 7-12 Sample Filter – Menu 21.3.1 7-14
Figure 7-13 Sample Filter Rules Summary - Menu 21.1 7-15
Figure 7-14 Filtering Ethernet Traffic 7-16
Figure 7-15 Filtering Remote Node Traffic 7-16
Figure 8-1 SNMP Management Model 8-1

Figure 8-2 Menu 22 – SNMP Configuration 8-3
Figure 9-1 Menu 24 - System Maintenance 9-1
Figure 9-2 Menu 24.1 – System Maintenance – Status 9-2
Figure 9-3 Menu 24.2 – System Information and Console Port Speed 9-3
Figure 9-4 Menu 24.2.1 – System Maintenance – Information 9-3
Figure 9-5 Menu 24.2.2 – System Maintenance – Change Console Port Speed 9-4
Figure 9-6 Menu 24.3 – System Maintenance – Log and Trace 9-5
Figure 9-7 Sample Error and Information Messages 9-5
Figure 9-8 Menu 24.3.2 – System Maintenance – Syslog 9-6
Figure 9-9 Menu 24.4 – System Maintenance – Diagnostic 9-7
Figure 10-1 Telnet in Menu 24.5 10-3
Figure 10-2 FTP Session Example 10-4
Figure 10-3 System Maintenance – Backup Configuration 10-6
Figure 10-4 System Maintenance – Starting Xmodem Download Screen 10-6
Figure 10-5 Backup Configuration Example 10-7
Figure 10-6 Successful Backup Confirmation Screen 10-7
Figure 10-7 Telnet into Menu 24.6 10-8
Figure 10-8 Restore Using FTP Session Example 10-9
Figure 10-9 System Maintenance – Restore Configuration 10-9
Figure 10-10 System Maintenance – Starting Xmodem Download Screen 10-9
Figure 10-11 Restore Configuration Example 10-10
Figure 10-12 Successful Restoration Confirmation Screen 10-10
Figure 10-13 Telnet Into Menu 24.7.1 – Upload System Firmware 10-11
Figure 10-14 Telnet Into Menu 24.7.2 – System Maintenance 10-11
Figure 10-15 FTP Session Example of Firmware File Upload 10-12
Figure 10-16 Menu 24.7.1 as seen using the Console Port 10-14
Figure 10-17 Example Xmodem Upload 10-14
Figure 10-18 Menu 24.7.2 as seen using the Console Port 10-15
Figure 10-19 Example Xmodem Upload 10-16
Figure 11-1 Menu 24 – System Maintenance 11-1
Figure 11-2 Valid CI Commands 11-1
Figure 11-3 Menu 24.10 System Maintenance – Time and Date Setting 11-2
Figure 12-1 Menu 26 - Schedule Setup 12-1
Figure 12-2 Schedule Set Setup 12-2
Figure 12-3 Applying Schedule Set(s) to a Remote Node (PPTP) 12-4
Figure 13-1 Telnet Configuration on a TCP/IP Network 13-1
Figure 13-2 Menu 24.11 - Remote Management Control 13-2

List of Tables

Table 2-1 Front Panel LED Description 2-2
Table 1-2 ZyAIR Wireless LAN Coverage 2-5
Table 2-3 Main Menu Commands 2-10
Table 2-4 Main Menu Summary 2-11
Table 2-5 General Setup Menu Fields 2-14
Table 2-6 Configure Dynamic DNS Menu Fields 2-15
Table 2-7 WAN Setup Field Descriptions 2-16
Table 3-1 DHCP Ethernet Setup Menu Fields 3-6
Table 3-2 TCP/IP Ethernet Setup Menu Fields 3-7
Table 3-3 IP Alias Setup Menu Fields 3-9
Table 3-4 Internet Account Information 3-11
Table 3-5 Internet Access Setup Menu Fields 3-12
Table 3-6 Wireless LAN Setup Field Description 3-16
Table 3-7 Roaming Configuration Field Descriptions 3-19
Table 4-1 Wireless LAN Setup Field Description 4-2
Table 4-2 IEEE802.1X System Security Field Descriptions 4-5
Table 4-3 Menu 23.2 System Security - External Server Field Description 4-6
Table 4-4 Menu 14.1- Edit Dial-in User Field Description 4-8
Table 4-5 MAC Address Filter Field Description 4-10
Table 5-1 Remote Node Profile Menu Fields 5-2
Table 5-2 Remote Node Network Layer Options 5-5
Table 5-3 Edit IP Static Route Menu Fields 5-9
Table 6-1 NAT Definitions 6-1
Table 6-2 NAT Mapping Types 6-5
Table 6-3 Applying NAT in Menus 4 & 11.3 6-7
Table 6-4 SUA Address Mapping Rules 6-9
Table 6-5 Fields in Menu 15.1.1 6-10
Table 6-6 Menu 15.1.1.1 - Editing/Configuring an Individual Rule in a Set 6-11
Table 6-7 Services & Port Numbers 6-13
Table 7-1 Abbreviations Used in the Filter Rules Summary Menu 7-5
Table 7-2 Rule Abbreviations Used 7-5
Table 7-3 TCP/IP Filter Rule Menu Fields 7-7
Table 7-4 Generic Filter Rule Menu Fields 7-11
Table 7-5 Filter Sets Table 7-15
Table 8-1 SNMP Configuration Menu Fields 8-3
Table 8-2 SNMP Traps 8-4
Table 8-3 Ports and Permanent Virtual Circuits 8-4
Table 9-1 System Maintenance – Status Menu Fields 9-2
Table 9-2 Fields in System Maintenance 9-3

Table 9-3 System Maintenance Menu – Syslog Parameters 9-6
Table 9-4 System Maintenance Menu – Diagnostic 9-7
Table 10-1 Filename Conventions 10-2
Table 10-2 General Commands for GUI-based FTP Clients 10-4
Table 10-3 General Commands for GUI-based TFTP Clients 10-6
Table 11-1 Time and Date Setting Fields 11-2
Table 12-1 Schedule Set Setup Fields 12-2
Table 13-1 Menu 24.11 -Remote Management Control 13-2
Table 14-1 Troubleshooting the Start-Up of Your ZyAIR 14-1
Table 14-2 Troubleshooting the Password 14-1
Table 14-3 Troubleshooting the Ethernet Interface 14-2
Table 14-4 Troubleshooting the WAN Interface 14-2
Table 14-5 Troubleshooting the Internet Access 14-3
Table 14-6 Troubleshooting Telnet 14-3

List of Diagrams

Diagram 1 Peer-to-Peer Communication in an Ad-hoc Network ..... B
Diagram 2 ESS Provides Campus-Wide Coverage C
Diagram 3 Sequences for EAP MD5-Challenge Authentication ..... F
Diagram 4 Single-PC per Modem Hardware Configuration I
Diagram 5 ZyAIR as a PPPoE Client ..... J
Diagram 6 Transport PPP frames over Ethernet ..... K
Diagram 7 PPTP Protocol Overview L
Diagram 8 Example Message Exchange between PC and an ANT L

Preface

The ZyAIR B-2000 Wireless LAN Gateway with 4-Port Switch is the ideal all-in-one device for small networks connecting to the Internet via a cable/DSL modem. The ZyAIR is equipped with four auto-sensing 10/100BASE-T Ethernet ports to connect to your network and an RJ-45 port to connect to your ADSL service.

The ZyAIR B-2000's 10/100M auto-negotiating LAN interface enables fast data transfer of either 10Mbps or 100Mbps in either half-duplex or full-duplex mode depending on your Ethernet network using either a crossover or straight-through Ethernet cable.

ZyAIR B-2000 has an embedded IEEE802.11b compliant 11Mpbs Ethernet wireless access point. It is suited for wireless connection to the wired network in the home and office environment allowing users to enjoy the convenience of wireless LAN access within the coverage area.

For security, your ZyAIR supports the latest IEEE802.1x standard, WEP (Wire Equivalent Privacy), and MAC address filtering.

Your ZyAIR is easy to install and configure. All functions are configurable via the SMT (System Management Terminal), embedded web configurator or the console port. Advanced users may configure the ZyAIR using CLI (Command Line Interface) commands.

Don’t forget to register your ZyAIR (fast, easy online registration at www.zyxel.com) for free future product updates and information.

About This User's Guide

This user's guide covers all aspects of ZyAIR operations and shows you how to get the best out of the multiple advanced features of your ZyAIR using the SMT. It is designed to guide you through the correct configuration of your ZyAIR for various applications.

Related Documentation

- Supporting Disk

  More detailed information and examples can be found in our included disk (as well as on the zyxel.com web site). This disk contains information on configuring your ZyAIR for Internet access, general and advanced FAQs, Application Notes, Troubleshooting, a reference for CI Commands and bundled software.

- Quick Installation Guide

  Our Quick Installation Guide is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.

- ZyXEL Web Site

The ZyXEL download library at www.zyxel.com contains additional support documentation. Please also refer to www.zyxel.com for an online glossary of networking terms.

Syntax Conventions

- "Type" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to use one predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- For brevity's sake, we will use "e.g.," as a shorthand for "for instance", and "i.e.," for "that is" or "in other words" throughout this manual.
- The ZyAIR B-2000 Wireless LAN Gateway with 4-Port Switch may be referred to as the ZyAIR B-2000 or, simply, as the ZyAIR in this user's guide.

Part I:

GETTING STARTED

This part is structured as a step-by-step guide to help you connect, install and set up your ZyAIR to operate on your network and to access the Internet. Described are Key Features and Application, Hardware Installation, Initial Setup and Internet Access.

Chapter 1
Getting To Know Your ZyAIR

This chapter describes the key features and applications of your ZyAIR.

1.1 ZyAIR B-2000 Wireless LAN Gateway with 4-Port Switch

The ZyAIR is a cost effective wireless LAN gateway with an integrated 10/100 Mbps and wireless interfaces and robust network management features for Internet access via an external cable/xDSL modem. Equipped with a 10Mbps Ethernet WAN port, four auto-negotiating 10/100Mbps Ethernet LAN ports and the Single User Account (SUA) feature, the ZyAIR is uniquely suited as a broadband Internet access-sharing gateway for multi-computer homes and home offices.

For added security, your ZyAIR supports various methods of network security: WEP, MAC address filtering, and IEEE 802.1x authentication.

ZyAIR provides ease of installation and superior network security. What's more, users enjoy the convenience and mobility with wireless LAN connectivity, working anywhere within the coverage area.

1.2 Features of the ZyAIR

Your ZyAIR is packed with a number of features that give it the flexibility to provide a complete networking solution for almost any user.

4-Port Switch

A combination of switch and router makes your ZyAIR a cost-effective and viable network solution. You can connect up to four computers to the LAN ports on you ZyAIR without the cost of a hub.

10/100M Auto-negotiation Ethernet/Fast Ethernet Interface

This auto-negotiation feature allows the ZyAIR to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

IEEE 802.11b 11 Mbps Wireless LAN

The 11 Mbps wireless LAN provides wireless mobility and a fast network environment for small and home offices. Computers with IEEE 802.11b wireless NICs (Network Interface Cards) can connect to the local area network without any wiring efforts and enjoy reliable high-speed connectivity.

Wireless LAN MAC Address Filtering

MAC Address Filtering together with ESSID (Extended Service Set IDentifier), WEP (Wired Equivalent Privacy) and IEEE 802.1x to ensure wireless network security.

IEEE 802.1x for Network Security

Your ZyAIR supports the IEEE 802.1x standard that works with the IEEE 802.11 to enhance user authentication. With the local user profile, the ZyAIR allows you to configure up 32 user profiles without a network authentication server. In addition, centralized user and accounting management is possible on an optional network authentication server.

EAP (RFC2284)

EAP (Extensible Authentication Protocol) supports multiple authentication methods to ensure the highest security level available.

RADIUS (RFC2138, 2139)

RADIUS (Remote Authentication Dial In User Service) server enables authentication, authorization and accounting for your wireless network.

PPPoE Support (RFC2516)

PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on the ZyAIR is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.

PPTP Support

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using a TCP/IP-based network. PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. Use PPTP to connect to a broadband modem to achieve access to high-speed data networks via a familiar "dial-up networking" user interface.

NAT for Single-IP-address Internet Access

The ZyAIR's SUA (Single User Account) feature allows multiple-user Internet access for the cost of a single IP account. NAT supports popular Internet applications such as MS traceroute, CuSeeMe, IRC, RealPlayer, VDOLive, Quake, and PPTP. No configuration is needed to support these applications.

Dynamic DNS Support

With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS client.

DHCP Support

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The ZyAIR has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. The ZyAIR also acts as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.

Multicast

Traditionally, IP packets are transmitted in two ways - unicast or broadcast. Multicast is a third way to deliver IP packets to a group of hosts. IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC 2236). The ZyAIR supports versions 1 and 2.

Network Management

- Menu driven SMT (System Management Terminal) management
- Embedded Web Configurator
- CLI (Command Line Interpreter)
- Remote SMT session via Telnet
- Remote Management via Telnet, FTP or Web servers.
- Console port management
- SNMP manageable
- DHCP Server/Client
- Built-in Diagnostic Tools
- Syslog
- Telnet Support (Password-protected telnet access to internal configuration manager)
- TFTP/FTP server, firmware upgrade and configuration backup/support supported

Diagnostics Capabilities

The ZyAIR can perform self-diagnostic tests. These tests check the integrity of the following circuitry:

- FLASH memory
- DRAM
- LAN port

- Wireless port

Ease of Installation

Your ZyAIR is designed for quick, intuitive and easy installation.

Housing

Your ZyAIR's all new compact and ventilated housing minimizes space requirements making it easy to position anywhere in your busy office.

1.3 Application for the ZyAIR

1.3.1 Broadband Internet Access via Cable or DSL modem.

A cable modem or DSL modem can be connected to the ZyAIR **WAN** port and up to four computers can be connected to the ZyAIR **LAN** ports for super-fast broadband Internet access. Wireless clients also enjoy the LAN connectivity to the Internet. The ZyAIR provides not only the high-speed Internet access but also a complete solution to efficiently manage data traffic on your network.

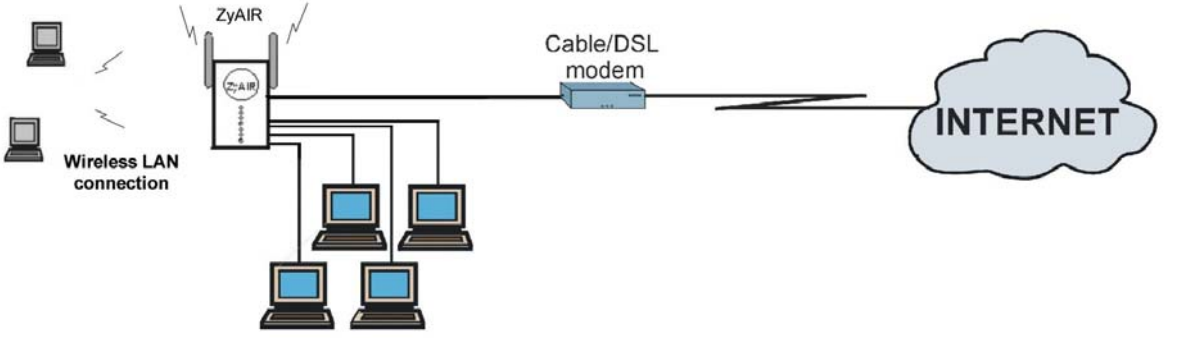

Figure 1-1 Internet Access Application

Chapter 2
Hardware Installation and Initial Setup

This chapter describes the physical features of the ZyAIR and how to make cable connections.

2.1 Front Panel LEDs of the ZyAIR

The LEDs on the front panel indicate the operational status of your ZyAIR

Figure 2-1 ZyAIR Front Panel

Table 2-1 Front Panel LED Description

LED	COLOR	STATUS	DESCRIPTION
LINK	Green	On	The wireless card on the ZyAIR is working.
		Off	The wireless card on the ZyAIR is not working.
ZyAIR (WLAN ACK)	Blue	On (dim)	The ZyAIR is ready, but is not sending/receiving data through the wireless LAN.
		Breathing	The ZyAIR is sending/receiving data through the wireless LAN.
LAN 1-4	Green	On	The ZyAIR has a successful 10Mb Ethernet connection.
		Blinking	The ZyAIR is sending/receiving data.
		Off	The ZyAIR does not have 10Mb Ethernet connection.
	Orange	On	The ZyAIR has a successful 100Mb Ethernet connection.
		Blinking	The ZyAIR is sending/receiving data.
		Off	The ZyAIR does not have 100Mb Ethernet connection.
WAN	Green	On	The ZyAIR has successful 10Mb WAN connection.
		Blinking	The ZyAIR is sending/receiving data.
		Off	The ZyAIR does not have 10Mb WAN connection.
	Orange	On	The ZyAIR has successful 100Mb WAN connection.
		Blinking	The ZyAIR is sending/receiving data.
		Off	The ZyAIR does not have 100Mb WAN connection.
SYS	Green	On	The ZyAIR is functioning properly.
		Blinking	The ZyAIR is rebooting.
		Off	The ZyAIR is not ready or has malfunctioned.
PWR	Green	On	The ZyAIR is receiving power.
		Off	The ZyAIR is not receiving power.

2.2 Side Panel and Connections of the ZyAIR

The following figure shows the side panel of your ZyAIR.

Figure 2-2 ZyAIR Side Panel and Connections

2.2.1 WAN Port

Connecting the ZyAIR to a Cable Modem

1. Connect the **WAN** port on the ZyAIR to the Ethernet port on your cable modem using the Ethernet cable that came with your cable modem. The Ethernet port on a cable modem is sometimes labeled "PC" or "Workstation".
2. Connect the coaxial cable from your cable service to the threaded coaxial cable connector on the back of the cable modem.

Connecting the ZyAIR to a DSL Modem

Connect the **WAN** port on the ZyAIR to the Ethernet port on your DSL modem using the Ethernet cable that came with your DSL modem.

2.2.2 Four LAN 10/100M Ports

Ethernet 10Base-T/100Base-T networks use Shielded Twisted Pair (STP) cable with RJ-45 connectors that look like a bigger telephone plug with 8 pins. All LAN ports are auto-sensing, so you may use the crossover cable provided or a straight-through Ethernet cable to connect your ZyAIR to a computer/external hub.

If you want to connect more than four computers to your ZyAIR, you must use an external hub. Connect a **LAN** port on the ZyAIR to a port on the hub using a crossover Ethernet cable.

When the ZyAIR is on and properly connected to a computer or a hub, the corresponding LAN **LED on the front panel turns on.**

2.2.3 Console Port

Use terminal emulator software on a computer for configuring your ZyAIR via the console port. Connect the 7-pin end of the supplied console cable to the console port of the ZyAIR and the 9-pin female end to a serial port (COM1, COM2 or other COM port) of your computer. See the section on *Additional Installation Requirements* to configure the terminal emulator software to log in to the ZyAIR through the console port.

2.2.4 Restore Factory Defaults/Reset Button

Reset to the factory defaults by holding the **RESET** button in for about 5 seconds to restart the ZyAIR .Refer to section *2.6* for information on the factory default values on your ZyAIR.

All custom settings will be lost once you reset to the default settings.

2.2.5 Power Port

Connect the power adapter to the port labeled **POWER** on the side panel of your ZyAIR which then automatically turns on.

The ZyAIR will reboot if the supplied power is too low. This is a normal operation.

To avoid damage to the ZyAIR, make sure you use the correct power adapter. Refer to the *Power Adapter Specification Appendix* for this information.

2.2.6 F.G. (Frame Ground)

Ground the ZyAIR by connecting a grounded wire to the F.G. terminal.

2.2.7 Antennas

The ZyAIR is equipped with two reverse SMA connectors and two detachable omni-directional 2dBi antennas to provide clear radio signal between the wireless stations and the access points. Refer to the *Antenna Selection and Positioning Recommendations* appendix for more information.

The following table shows the ZyAIR's coverage in meters using the included antennas. The distance may differ depending on the network environment.

Table 1-2 ZyAIR Wireless LAN Coverage

	≈11 Mbps	≤ 5.5 Mbps
Indoor	50 m	80 m
Outdoor	200 m	300 m

ZyXEL offers several optional antennas to provide optimum coverage and performance for your ZyAIR.

Refer to the *Quick Start Guide* for instructions to attach the antennas to your ZyAIR.

2.3 Hardware Mounting Options

The ZyAIR may be placed on a flat surface or wall mounted.

In general, the best location to place the access point is at the center of your intended wireless coverage area. For better performance, mount the ZyAIR in a high position free of obstructions.

Refer to the *Quick Start Guide* for hardware installation procedure.

2.4 Additional Installation Requirements

- A computer with an IEEE 802.11b wireless LAN card or an Ethernet 10Base-T/100Base-T NIC.
- To enable remote RADIUS authentication for wireless clients, you need
  - A wireless client computer running IEEE 802.1x-compliant software. Currently, this is offered in Windows XP.
  - A network RADIUS server for remote user authentication and accounting.
- A computer equipped with a web browser (with JavaScript enabled) and/or Telnet.
- A computer equipped with communications software (for example, Hyper Terminal in Windows) configured to the following parameters:
  - VT100 terminal emulation.
  - 9600 baud rate.
  - Parity set to none, 8 data bits, 1 stop bit.
  - Flow control set to none.
- A cable/xDSL modem and an ISP account for Internet access.

2.5 ZyAIR Configuration

Configure your ZyAIR using:

- Web configurator
- SMT (System Management Terminal). Access the SMT via:
  - LAN or WAN using Telnet
  - Console port using terminal emulation software

2.5.1 Connect to Your ZyAIR Using the Web Configurator

Step 1. Make sure your computer IP address and the ZyAIR IP address are on the same subnet. Refer to the *TCP/IP* appendix.

Step 2. Launch your web browser and enter 192.168.1.1 as the URL.

Step 3. In the **Password** field, type "1234". Click **Login**.

Step 4. Either enter a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Click the **Help** button for online web configurator HTML help.

2.5.2 Connect to your ZyAIR Using Telnet

The following procedure details how to telnet into your ZyAIR.

Step 1. Make sure your computer IP address and the ZyAIR IP address are on the same subnet. Refer to the *TCP/IP* appendix.

Step 2. In Windows, click **Start** (usually in the bottom left corner), **Run** and then type “telnet 192.168.1.1” (the default IP address) and click **OK**.

Step 3. Enter 1234 in the **Password** field.

Step 4. After entering the password you will see the main menu.

2.5.3 Connect to Your ZyAIR Using the Console Port

Step 1. Connect the 7-pin male end of a console port cable to the port labelled **CONSOLE** on the ZyAIR and the 9-pin female end to an avaliable serial port on your computer.

Step 2. Run the communications software and configure the communication parameteres as described in the *Additional Installation Requirements* section.

Step 3. Turn on your ZyAIR and you should see the initial screen shown next.

Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your ZyAIR will automatically log you out.

The remainder of this user's guide shows you how to configure the ZyAIR for Internet access using SMT screens through the console port. There are also some sections in this guide that focus on using Telnet to configure the ZyAIR.

2.5.4 Initial Screen

When you turn on your ZyAIR, it performs several internal tests as well as line initialization. After the initialization, the ZyAIR asks you to press [ENTER] to continue, as shown.

```
Copyright (c) 1994 - 2002 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:A0:C5:00:15:37
initialize ch =1, ethernet address: 00:A0:C5:00:15:38
initialize ch =2, ethernet address: 00:A0:C5:00:15:37
Press ENTER to continue...
```

Figure 2-3 Power-On Display

2.5.5 Entering Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown next.

For your first login, enter the default password "1234". As you type the password, the screen displays an "x" for each character you type.

Please note that if there is no activity for longer than five minutes after you log in, your ZyAIR will automatically log you out and will display a blank screen. If you see a blank screen, press [ENTER] to display the login screen again.

```
Enter Password : xxxx
```

Figure 2-4 Login Screen

2.6 Resetting the ZyAIR

If you forget your password or cannot access the ZyAIR, you will need to reload the factory-default configuration file. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously; the password will be reset to "1234" and the LAN IP address to 192.168.1.1.

To obtain the default configuration file, download it from the ZyXEL FTP site, unzip it and save it in a folder.

2.6.1 Methods of Restoring Factory-Defaults

You can erase the current configuration and restore factory defaults in three ways:

1. Transfer the configuration file to your ZyAIR using the SMT menus. See later in this User's Guide for more information on this.
2. Use the **RESET** button on the side panel of the ZyAIR to upload the default configuration file (hold this button in for more than 3 seconds). Use this method for cases when the password or IP address of the ZyAIR is not known.
3. Use the web configurator to restore defaults (see the web configurator HTML help)

All custom settings will be lost once you reset to the default settings.

2.6.2 ZyAIR SMT Menu Overview

The following figure gives you an overview of the various SMT menu screens of your ZyAIR.

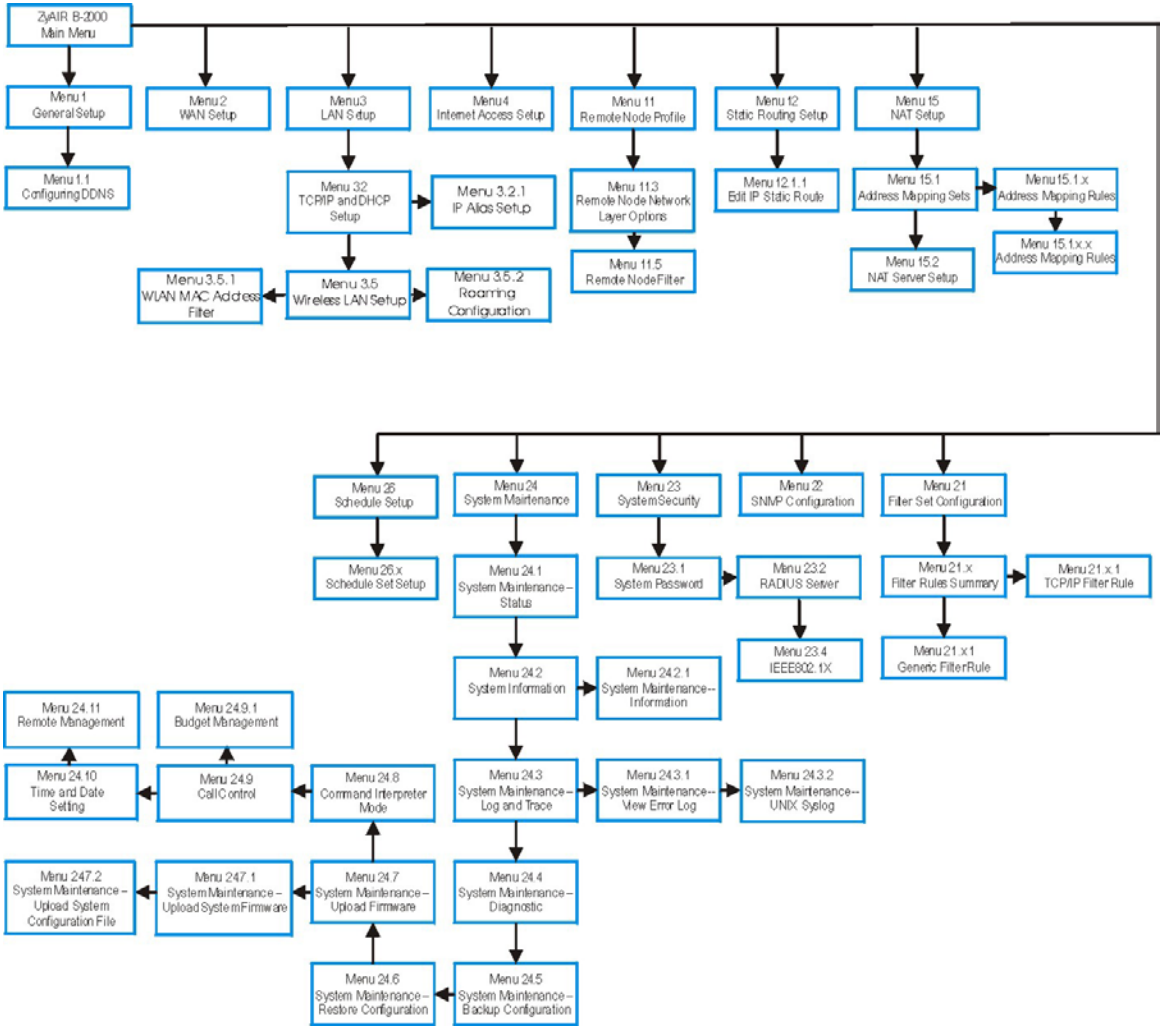
ZyAIR B-2000 Main Menu
Menu 1 General Setup
Menu 1.1 Configuring DDNS
Menu 2 WAN Setup
Menu 3 LAN Setup
Menu 3.2 TCP/IP and DHCP Setup
Menu 3.2.1 IP Alias Setup
Menu 3.5 Wireless LAN Setup
Menu 3.5.1 WLAN MAC Address Filter
Menu 3.5.2 Roaming Configuration
Menu 4 Internet Access Setup
Menu 11 Remote Node Profile
Menu 11.3 Remote Node Network Layer Options
Menu 11.5 Remote Node Filter
Menu 12 Static Routing Setup
Menu 12.1.1 Edit IP Static Route
Menu 15 NAT Setup
Menu 15.1 Address Mapping Sets
Menu 15.1.x Address Mapping Rules
Menu 15.1.x.x Address Mapping Rules
Menu 15.2 NAT Server Setup
Menu 25 Schedule Setup
Menu 25.x Schedule Set Setup
Menu 24 System Maintenance
Menu 24.1 System Maintenance – Status
Menu 24.2 System Information
Menu 24.2.1 System Maintenance – Information
Menu 24.3 System Maintenance – Log and Trace
Menu 24.3.1 System Maintenance – View Error Log
Menu 24.3.2 System Maintenance – UNIX Syslog
Menu 24.4 System Maintenance – Diagnostic
Menu 24.5 System Maintenance – Backup Configuration
Menu 24.6 System Maintenance – Restore Configuration
Menu 24.7 System Maintenance – Upload Firmware
Menu 24.7.1 System Maintenance – Upload System Firmware
Menu 24.7.2 System Maintenance – Upload System Configuration File
Menu 24.8 Command Interpreter Mode
Menu 24.9 Call Control
Menu 24.9.1 Budget Management
Menu 24.10 Time and Date Setting
Menu 24.11 Remote Management
Menu 23 System Security
Menu 23.1 System Password
Menu 23.2 RADIUS Server
Menu 23.4 IEEE802.1X
Menu 22 SNMP Configuration
Menu 21 Filter Set Configuration
Menu 21.x Filter Rules Summary
Menu 21.x.1 TCP/IP Filter Rule
Menu 21.x.1 Generic Filter Rule

Figure 2-5 ZyAIR SMT Menu Overview

2.7 Navigating the SMT Interface

The SMT (System Management Terminal) is the interface that you use to configure your ZyAIR.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 2-3 Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.
Move to a “hidden” menu	Press [SPACE BAR] to change **No** to **Yes** then press [ENTER].	Fields beginning with “Edit” lead to hidden menus and have a default setting of **No**. Press [SPACE BAR] once to change **No** to **Yes**, then press [ENTER] to go to the “hidden” menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys.	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Entering information	Type in or press [SPACE BAR], then press [ENTER].	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<?>	All fields with the symbol <?> must be filled in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message “Press ENTER to confirm or ESC to cancel”. Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

After you enter the password, the SMT displays the main menu, as shown next.

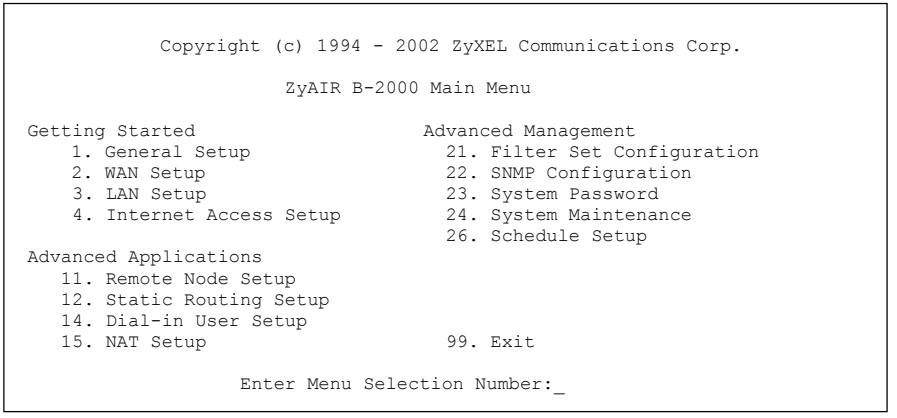

Figure 2-6 SMT Main Menu

The SMT menu continually improves and changes with new firmware upgrades. Check the release notes at www.zyxel.com to find the most recent upgrades and information.

2.7.1 System Management Terminal Interface Summary

Table 2-4 Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
2	WAN	Use this menu to set up your WAN connection.
3	LAN Setup	Use this menu to set up your LAN and WLAN connection.
4	Internet Access Setup	A quick and easy way to set up an Internet connection.
11	Remote Node Setup	Use this menu to set up the Remote Node for LAN-to-LAN connection, including Internet connection.
12	Static Routing Setup	Use this menu to set up static routes.
14	Dial-in User Setup	Use this menu to set up local user profiles on the ZyAIR.
15	NAT Setup	Use this menu to specify inside servers when NAT is enabled.
21	Filter Set Configuration	Use this menu to set up filters to provide security, etc.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Password	Use this menu to change your password.

Table 2-4 Main Menu Summary

#	MENU TITLE	DESCRIPTION
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
26	Schedule Setup	Use this menu to schedule outgoing calls.
99	Exit	Use this to exit from SMT and return to a blank screen.

2.8 Changing the System Password

Change the ZyAIR default password by following the steps shown next.

Step 1. Enter 23 in the main menu to display **Menu 23 - System Password** as shown next.

Step 2. Type your existing system password in the **Old Password** field, for example "1234", and press [ENTER].

```
                Menu 23 - System Password

        Old Password= ****
        New Password= ?
        Retype to confirm= ?


         Enter here to CONFIRM or ESC to CANCEL:
```

Figure 2-7 Menu 23 – System Password

Step 3. Type your new system password in the **New Password** field (up to 30 characters), and press [ENTER].

Step 4. Re-type your new system password in the **Retype to confirm** field for confirmation and press [ENTER].

Note that as you type a password, the screen displays an asterisk "*" for each character you type.

2.9 General Setup

Menu 1 – General Setup contains administrative and system-related information (shown next). The **System Name** field is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start**, **Settings Control**, **Panel Network**. Click the **Identification** tab, note the entry for the **Computer name** field and enter it as the ZyAIR **System Name**.

In Windows 2000 click **Start, Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the ZyAIR **System Name**.

In Windows XP, click **start**, **My Computer View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyAIR **System Name**.

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the ZyAIR via DHCP.

2.9.1 Dynamic DNS

Dynamic DNS (Domain Name System) allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe or other services). You can also access your FTP server or Web site on your own computer using a DNS-like address (for example, myhost.dhs.org, where myhost is a name of your choice) which will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a DNS name.

To use this service, you must register with the Dynamic DNS service provider. The Dynamic DNS service provider will give you a password or key. The ZyAIR supports www.dyndns.org. You can apply to this service provider for Dynamic DNS service.

DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

2.9.2 Procedure To Configure Menu 1

Step 1. Enter 1 in the Main Menu to open **Menu 1 – General Setup** (shown next).

```
                Menu 1 - General Setup

        System Name= ?
        Domain Name=
        Edit Dynamic DNS= No

         Press ENTER to Confirm or ESC to Cancel:
```

Figure 2-8 Menu 1 – General Setup

Step 2. Fill in the required fields. Refer to the table shown next for more information about these fields.

Table 2-5 General Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
System Name	Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.	ZyAIR
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domainname" to see the current domain name used by your gateway. If you want to clear this field just press the [SPACE BAR]. The domain name entered by you is given priority over the ISP assigned domain name.	zyxel.com.tw
Edit Dynamic DNS	Press [SPACE BAR] to select **Yes** and press [ENTER] to configure **Menu 1.1 – Configure Dynamic DNS** (discussed next).	**No**
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

2.9.3 Procedure to Configure Dynamic DNS

If you have a private WAN IP address, then you cannot use Dynamic DNS.

Step 1. To configure Dynamic DNS, go to **Menu 1 – General Setup** and select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1– Configure Dynamic DNS** as shown next.

```
                Menu 1.1 - Configure Dynamic DNS

        Service Provider= WWW.DynDNS.ORG
        Active= Yes
        DDNSType= DynamicDNS
        Host=
        EMAIL=
        USER=
        Password= ********
        Enable Wildcard= No
        Offline= N/A

               Press ENTER to Confirm or ESC to Cancel:
```

Figure 2-9 Configure Dynamic DNS

Follow the instructions in the next table to configure Dynamic DNS parameters.

Table 2-6 Configure Dynamic DNS Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Service Provider	This is the name of your Dynamic DNS service provider.	WWW.DynDNS.ORG (default)
Active	Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active.	**Yes**
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.	**Dynamic DNS** (default)
Host	Enter the domain name assigned to your ZyAIR by your Dynamic DNS provider.	me.dyndns.org
EMAIL	Enter your e-mail address.	mail@mailserver
USER	Enter your user name.	
Password	Enter the password assigned to you.	
Enable Wildcard	Your ZyAIR supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select **Yes** to activate wildcard. This field is **N/A** when you choose DDNS client as your service provider.	**No**
Offline	This option is available when **CustomDNS** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.	**N/A**
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

2.10 WAN Setup

The MAC address field allows users to configure the WAN port's MAC Address by either using the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different rom file.

ZyXEL recommends you clone the MAC address from a workstation on your LAN even if your ISP does not require MAC address authentication.

From the main menu, enter 2 to display **Menu 2-WAN Setup** screen as shown.

```
                    Menu 2 - WAN Setup

                  MAC Address:
                    Assigned By= Factory default
                    IP Address= N/A


              Press ENTER to Confirm or ESC to Cancel:
```

Figure 2-10 Menu 2 – WAN Setup

The following table describes the fields in this screen.

Table 2-7 WAN Setup Field Descriptions

FIELD	DESCRIPTION	EXAMPLE
MAC Address		
Assigned By	Press [SPACE BAR] to select **Factory default** and press [ENTER] to use the factory assigned MAC address. Select **IP address attached on LAN** and enter the IP address in the **IP Address** field below to clone the MAC address of the computer on the Ethernet.	**Factory default**
IP Address	Enter the IP address of the computer whose MAC address you are cloning. This field is available if you select **IP address attached on LAN** in the **Assigned By** field.	N/A

2.11 LAN Setup

This section describes how to configure the Ethernet using **Menu 3** – **LAN Setup**. From the main menu, enter 3 to display menu 3.

```
                    Menu 3 - LAN Setup

          1. LAN Port Filter Setup
          2. TCP/IP and DHCP Setup


          5. Wireless LAN Setup

                Enter Menu Selection Number:
```

Figure 2-11 Menu 3 – LAN Setup

Detailed explanation about the LAN Setup screens is given in the next chapter.

2.11.1 General Ethernet Port Filter Setup

This menu allows you to specify filter set(s) that you wish to apply to the Ethernet traffic. You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches.

```
                Menu 3.1 - LAN Port Filter Setup

          Input Filter Sets:
            protocol filters=
            device filters=
          Output Filter Sets:
            protocol filters=
            device filters=

          Press ENTER to Confirm or ESC to Cancel:
```

Figure 2-12 Menu 3.1 – General Ethernet Setup

If you need to define filters, please read the *Filter Set Configuration* chapter first, then return to this menu to define the filter sets.

Chapter 3
Internet Access

This chapter shows you how to configure the LAN and WAN of your ZyAIR for Internet access.

3.1 Factory Ethernet Defaults

The Ethernet parameters of the ZyAIR are preset in the factory with the following values:

1. Ethernet IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits).
2. DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If the parameters are satisfactory, you can skip to *TCP/IP Ethernet Setup and DHCP* to enter the DNS server address(es) if your ISP gives you explicit DNS server address(es). If you wish to change the factory defaults or to learn more about TCP/IP, please read on.

3.2 LANs and WANs

A LAN (Local Area Network) is a computer network limited to the immediate area, usually the same building or floor of a building. A WAN (Wide Area Network), on the other hand, is an outside connection to another network or the Internet.

3.2.1 LANs, WANs and the ZyAIR

The actual physical connection determines whether the ZyAIR ports are LAN or WAN ports. There are two separate IP networks, one inside, the LAN network; the other outside: the WAN network as shown next:

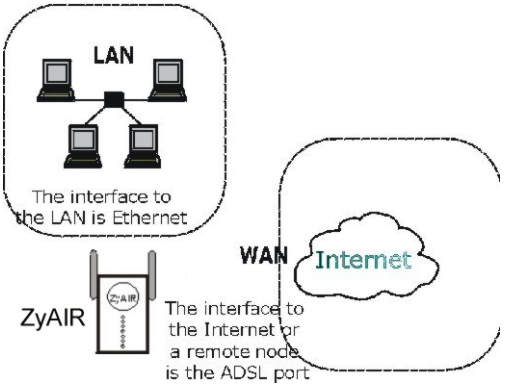
LAN
The interface to the LAN is Ethernet
WAN
Internet
ZyAIR
The interface to the Internet or a remote node is the ADSL port

Figure 3-1 LAN & WAN IPs

3.3 TCP/IP Parameters

3.3.1 IP Address and Subnet Mask

Like houses on a street that share a common street name, the computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 (ignoring the trailing zero) and you must enable the Single User Account feature of the ZyAIR. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do *not* use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.154 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

The subnet mask specifies the network number portion of an IP address. Your ZyAIR will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyAIR unless you are instructed to do otherwise.

3.3.2 Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

```
10.0.0.0     –  10.255.255.255

172.16.0.0   –  172.31.255.255

192.168.0.0  –  192.168.255.255
```

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

3.3.3 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

1. **Both -** the ZyAIR will broadcast its routing table periodically and incorporate the RIP information that it receives.
2. **In Only -** the ZyAIR will not send any RIP packets but will accept all RIP packets received.
3. **Out Only -** the ZyAIR will send out RIP packets but will not accept any RIP packets received.
4. **None -** the ZyAIR will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the ZyAIR sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but RIP-2 carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.

3.3.4 DHCP Configuration

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The ZyAIR has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. The ZyAIR can also act as a surrogate DHCP server where it relays IP address assignment from the actual DHCP server to the clients.

IP Pool Setup

The ZyAIR is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64 for the client machines. This leaves 31 IP addresses, 192.168.1.3 to 192.168.1.32 (excluding the ZyAIR itself which has a default IP of 192.168.1.1) for other server machines, for example, server for mail, FTP, telnet, web, etc., that you may have.

DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, for example, the IP address of *www.zyxel.com* is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. If your ISP does give you the DNS server addresses, enter them in the **DNS Server** fields in **DHCP Setup**, otherwise, leave them blank.

Some ISP's choose to pass the DNS servers using the DNS server extensions of PPP IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The ZyAIR supports the IPCP DNS server extensions through the DNS proxy feature.

If the **Primary** and **Secondary DNS Server** fields in **DHCP Setup** are not specified, for instance, left as 0.0.0.0, the ZyAIR tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the ZyAIR, the ZyAIR forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** menu. This way, the ZyAIR can pass the DNS servers to the computers and the computers can query the DNS server directly without the ZyAIR's intervention.

3.4 IP Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender – 1 recipient) or Broadcast (1 sender – everybody on the network). Multicast is a third way to deliver IP packets to *a group* of hosts on the network - not everybody.

IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The ZyAIR supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). At start up, the ZyAIR queries all directly connected networks to gather group membership. After that, the ZyAIR periodically updates this information. IP Multicasting can be enabled/disabled on the ZyAIR LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN). Select **None** to disable IP Multicasting on these interfaces.

3.5 TCP/IP Ethernet and DHCP Setup

Use menu 3.2 to configure your ZyAIR for TCP/IP.

To edit menu 3.2, enter 3 from the main menu to display **Menu 3-Ethernet Setup**. When menu 3 appears, press 2 and press [ENTER] to display **Menu 3.2-TCP/IP and DHCP Ethernet Setup**, as shown next:

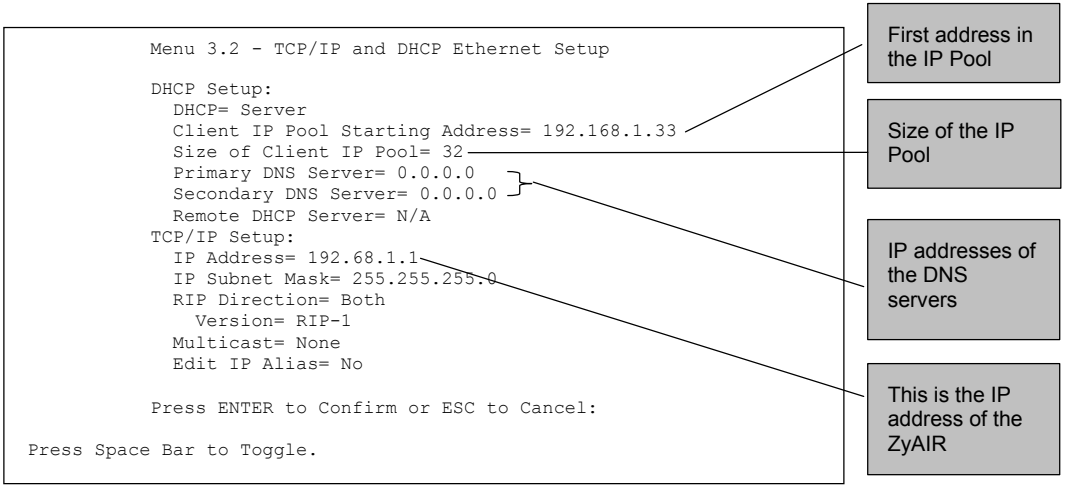
Menu 3.2 - TCP/IP and DHCP Ethernet Setup
DHCP Setup:
DHCP= Server
Client IP Pool Starting Address= 192.168.1.33
Size of Client IP Pool= 32
Primary DNS Server= 0.0.0.0
Secondary DNS Server= 0.0.0.0
Remote DHCP Server= N/A
TCP/IP Setup:
IP Address= 192.68.1.1
IP Subnet Mask= 255.255.255.0
RIP Direction= Both
Version= RIP-1
Multicast= None
Edit IP Alias= No
Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
First address in the IP Pool
Size of the IP Pool
IP addresses of the DNS servers
This is the IP address of the ZyAIR

Figure 3-2 Menu 3.2 – TCP/IP and DHCP Ethernet Setup

Follow the instructions in the following table on how to configure the DHCP fields.

Table 3-1 DHCP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
DHCP Setup DHCP	If set to **Server**, your ZyAIR can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to **None**, the DHCP server will be disabled. If set to **Relay**, the ZyAIR acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server in this case. When DHCP is used, the following items need to be set:	**Server** (default)
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size or count of the IP address pool.	32
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	

Table 3-1 DHCP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Remote DHCP Server	If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here.	

Follow the instructions in the following table to configure TCP/IP parameters for the Ethernet port.

Table 3-2 TCP/IP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
TCP/IP Setup		
IP Address	Enter the (LAN) IP address of your ZyAIR in dotted decimal notation	192.168.1.1
IP Subnet Mask	Your ZyAIR will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyAIR.	255.255.255.0
RIP Direction	Press [SPACE BAR] to select the RIP direction. Choices are **Both**, **In Only**, **Out Only** or **None**.	**Both** (default)
Version	Press [SPACE BAR] to select the RIP version. Choices are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1** (default)
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyAIR supports both IGMP version 1(**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** to disable it.	**None** (default)
Edit IP Alias	The ZyAIR supports three logical LAN interfaces via its single physical Ethernet interface with the ZyAIR itself as the gateway for each LAN network. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to menu 3.2.1	**No** (default)
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

3.6 IP Alias

IP Alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyAIR supports three logical LAN interfaces via its single physical Ethernet interface with the ZyAIR itself as the gateway for each LAN network.

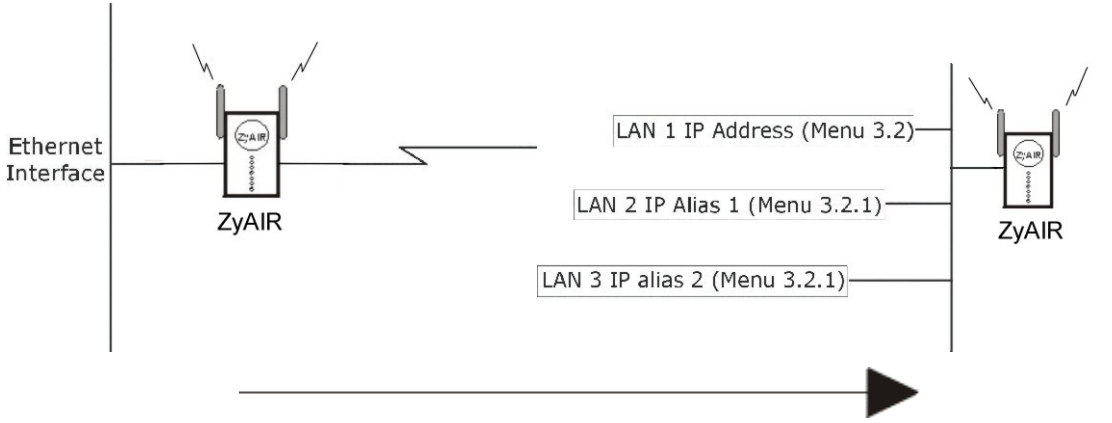

Figure 3-3 Physical Network **Figure 3-4 Partitioned Logical Networks**

Use menu 3.2.1 to configure IP Alias on your ZyAIR.

3.6.1 IP Alias Setup

Use menu 3.2 to configure the first network. Move the cursor to **Edit IP Alias** field and press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

```
Menu 3.2 - TCP/IP and DHCP Setup

DHCP Setup:
 DHCP= Server
 Client IP Pool Starting Addres= 192.168.1.33
 Size of Client IP Pool= 6
 Primary DNS Server= 0.0.0.0
 Secondary DNS Server= 0.0.0.0
 Remote DHCP Server= N/A
TCP/IP Setup:
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= None
    Version= N/A
  Multicast= None
  IP Policies=
  Edit IP Alias= Yes

Press ENTER to confirm or ESC to Cancel:
```

Figure 3-5 Menu 3.2-TCP/IP and DHCP Setup

Press [ENTER] to display **Menu 3.2.1-IP Alias Setup**, as shown next.

```
                Menu 3.2.1 - IP Alias Setup

        IP Alias 1= No
          IP Address= N/A
          IP Subnet Mask= N/A
          RIP Direction= N/A
            Version= N/A
          Incoming protocol filters= N/A
          Outgoing protocol filters= N/A
        IP Alias 2= No
          IP Address= N/A
          IP Subnet Mask= N/A
          RIP Direction= N/A
            Version= N/A
          Incoming protocol filters= N/A
          Outgoing protocol filters= N/A

         Enter here to CONFIRM or ESC to CANCEL:
```

Figure 3-6 Menu 3.2.1-IP Alias Setup

Follow the instructions in the table below to configure IP Alias parameters.

Table 3-3 IP Alias Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
IP Alias	Choose **Yes** to configure the LAN network for the ZyAIR.	**Yes**
IP Address	Enter the IP address of your ZyAIR in dotted decimal notation	192.168.1.1
IP Subnet Mask	Your ZyAIR will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyAIR	255.255.255.0
RIP Direction	Press [SPACE BAR] to select the RIP direction. Choices are **None**, **Both**, **In Only** or **Out Only**.	**None**
Version	Press [SPACE BAR] to select the RIP version. Choices are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1**
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the ZyAIR.	
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the ZyAIR.	
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

3.7 Encapsulation

Be sure to use the encapsulation method required by your ISP. The ZyAIR supports the following methods.

3.7.1 Ethernet

This encapsulation method is used when the WAN port is used as a regular Ethernet.

3.7.2 PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF Draft standard specifying how a host personal computer interacts with a broadband modem (for example, xDSL, cable, wireless, etc.) to achieve access to high-speed data networks. It preserves the existing Microsoft Dial-Up Networking experience and requires no new learning or procedures.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example, Radius). For the user, PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for specific users.

Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyAIR (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the Teledat Router 400 does that part of the task. Furthermore, with SUA, all of the LAN's computers will have access. For more information on PPPoE, please refer to the *PPPoE Appendix*.

3.7.3 PPTP

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. For more information on PPTP, please refer to the *PPTP Appendix*.

3.8 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP Address.

3.9 Internet Access Configuration

Menu 4 allows you to enter the Internet Access information in one screen. Menu 4 is actually a simplified setup for one of the remote nodes that you can access in menu 11. Before you configure your ZyAIR for Internet access, you need to collect your Internet account information from your ISP and telephone company.

Use the following table to record your Internet Account Information. Note that if you are using PPP or PPPoE encapsulation, then the only ISP information you need is a login name and password.

Table 3-4 Internet Account Information

FIELD	DESCRIPTION	YOUR INFO
System Name	Name of the ZyAIR (optional).	
Service Name (PPPoE)	Enter the PPPoE service name if the ISP supplies one. Enter "any" if the ISP does not assign you one.	
Encapsulation	**Ethernet**, **PPPoE** or **PPTP**	
My Login	Enter the login name assigned by your ISP (for PPP/PPPoE only).	
My Password	Enter the password associated with your ISP assigned **My Login** (for PPP/PPPoE only).	
Idle Timeout (PPPoE or PPP)	Enter the time lapse, in seconds, before you automatically disconnect from the PPPoE or PPP server.	
IP Address	Enter if your IP address is not dynamically assigned.	
Network Address Translation	**Full Feature**, **SUA Only** or **None**.	
DNS Server Address Assignment	**Primary DNS server** **Secondary DNS server** Enter when using RFC 1483 Encapsulation or a static IP address.	

3.10 Internet Access Setup

From the main menu, type 4 to display **Menu 4 – Internet Access Setup**, as shown next.

```
                Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= Ethernet
  Service Type= Standard
  My Login= N/A
  My Password= N/A
  Login Server= N/A

IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= SUA Only

Press ENTER to Confirm or ESC to Cancel:
```

Figure 3-7 Internet Access Setup

The following table contains instructions on how to configure your ZyAIR for Internet access.

Table 3-5 Internet Access Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
ISP's Name	Enter the name of your Internet Service Provider. This information is for identification purposes only.	MyISP
Encapsulation	Press [SPACE BAR] to select the method of encapsulation used by your ISP. Choices are **PPPoE**, **PPP** or **Ethernet**.	**Ethernet**
Service Type	This field is available if you select the **Ethernet** encapsulation. Press [SPACE BAR] to select the service type then press [ENTER]. Choose a RoadRunner flavor if your ISP is using Time Warner's RoadRunner; otherwise choose **Standard**. The **User Name**, **Password** and **Login Server** fields are not applicable (N/A) for the latter. Choose from **Standard**, **Telstra** (RoadRunner Telstra or BigPond authentication method), **RR-Manager** (RoadRunner Manager authentication method) or **RR-Toshiba** (RoadRunner Toshiba authentication method).	**Standard**

Table 3-5 Internet Access Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
My Login	Configure the **My Login** and **My Password** fields for PPP and PPPoE encapsulation only. Enter the login name that your ISP gives you. If you are using PPPoE encapsulation**,** then this field must be of the form user@domain where domain identifies your PPPoE service name.	N/A
My Password	Enter the password associated with the login name above.	N/A
Login Server	Enter the IP address of the login server in dotted decimal notation.	10.11.12.13
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select **Static** or **Dynamic** address assignment.	Static
IP Address	Enter the IP address supplied by your ISP if applicable.	10.11.12.20
IP Subnet Mask	Your ZyAIR will automatically calculate the subnet mask based on the IP address that you entered. Unless you are implementing subnetting, use the subnet mask computed by the ZyAIR.	
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyAIR that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyAIR.	
Network Address Translation	Press [SPACE BAR] and then [ENTER] to select **None**, **SUA Only** or **Full Feature**. Please see the *NAT Chapter* for more details.	**SUA Only**
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

If all your settings are correct your ZyAIR should connect automatically to the Internet. If the connection fails, note the error message that you receive on the screen and take the appropriate troubleshooting steps.

3.11 Wireless LAN

3.11.1 Wireless LAN Parameters

Channel

The range of radio frequencies used by IEEE 802.11b wireless devices is called a channel. You can choose the radio channel depending on your geographical area. Adjacent Access Points (APs) with overlapping coverage areas should use different channels to reduce crosstalk. Crosstalk occurs when the radio signals from access points overlap and interfere one another degrading performance.

ESS ID

Extended Service Set (ESS) is defined as one or more access points (APs) acting as a bridge between a wired LAN and the associated wireless clients. The ESS ID is a unique ID given to the APs and the wireless clients that participate in the same wireless network. You can think the EES ID as being similar to a workgroup name in a Microsoft network.

Wireless LANs can be as simple as two computers with wireless network interface cards (NICs) communicating in a peer-to-peer network or as complex as a number of computers with wireless NICs communicating through access points which bridge network traffic to the wired LAN.

The ESS ID provides minimum security for your network, see section on *Wireless Security Setup* for more information.

RTS Threshold

The RTS (Request To Send) Threshold prevents the hidden node problem. Hidden node problem occurs when two stations are within the range of the same access point, but are not within the range of each other. The following figure illustrates the hidden node problem. Both stations (STA) are within the range of the AP, however, they cannot hear each other. Therefore, they are considered as hidden nodes from each other. When a station starts data transmission with the access point, it might not know that the other station is already using the wireless medium. When these two stations send data at the same time, they might collide when arriving simultaneously at the AP. The collision will most certainly result in a loss of messages for both stations.

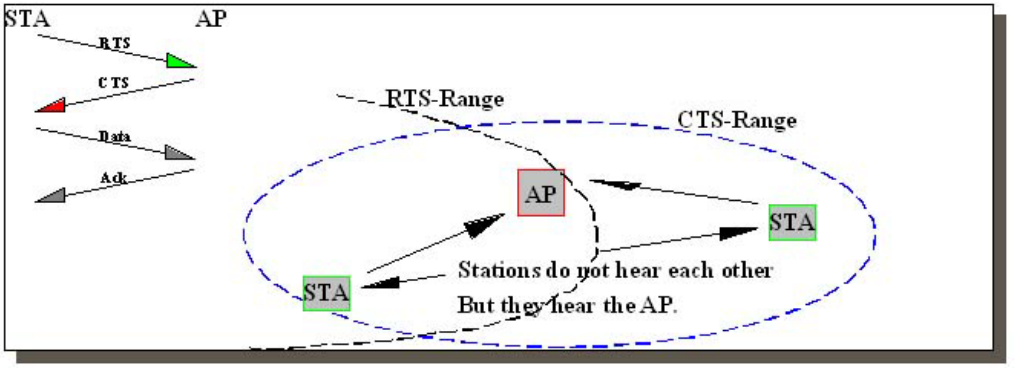

Figure 3-8 RTS Threshold

Thus, RTS Threshold mechanism provides a solution to prevent data collisions. When you enable RTS Threshold on a possible hidden station, this station and its AP will use a Request to Send/Clear to Send protocol (RTS/CTS). The station will send an RTS message to the AP, informing that it is going to transmit the data. Upon receipt, the Access Point will respond with a CTS message to all stations within its range to

notify all other stations to defer transmission. It will also confirm with the requesting station that the AP has reserved it for the time frame of the requested transmission.

The RTS function will be activated if the packet size exceeds the value you set. It is highly recommended that you set the value ranging from 0 to 2432.

Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

Fragmentation improves the efficiency when high traffic flows along in the wireless network.

WEP

As the first line of protection against wireless network intrusion, the ZyAIR provides the standard WEP (Wired Equivalent Privacy) for data encryption. However, there may be a significant degradation of the data throughput on the wireless link when WEP is enabled. See section on *Wireless Security Setup* for more information about configuring WEP data encryption.

3.11.2 Wireless LAN Setup

Use menu 3.5 to set up your ZyAIR as the wireless access point. To edit menu 3.5, enter 3 from the main menu to display **Menu 3 – LAN Setup**. When menu 3 appears, press 5 and then press [ENTER] to display **Menu 3.5 – Wireless LAN Setup** as shown next.

```
                Menu 3.5 - Wireless LAN Setup

ESSID= Wireless
Hide ESSID= No
Channel ID= CH01 2412MHz
RTS Threshold= 2432
Frag. Threshold= 2432
WEP= Disable
  Default Key= N/A
  Key1= N/A
  Key2= N/A
  Key3= N/A
  Key4= N/A
Edit MAC Address Filter= No
Edit Roaming Configuration= Yes

Press ENTER to Confirm or ESC to Cancel:
```

Figure 3-9 Menu 3.5 - Wireless LAN Setup

The following table describes the fields in this screen.

Table 3-6 Wireless LAN Setup Field Description

FIELD	DESCRIPTION	EXMAPLE
ESSID	The ESSID (Extended Service Set IDentity) identifies the AP the wireless client is to associate to. Wireless clients associating to the AP must have the same ESSID. Enter a descriptive name up to 32 printable 7-bit ASCII characters.	**Wireless**
Hide ESSID	Press [SPACE BAR] and select **Yes** to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning.	**No**
Channel ID	Press [SPACE BAR] to select a channel. This allows you to set the operating frequency/channel depending on your particular region. Possible choices are **CH01 2412MHz**, **CH02 2417MHz**, **CH03 2422MHz, CH04 2427MHz**, **CH05 2432MHz**, **CH06 2437MHz**, **CH07 2442MHz**, **CH08 2447MHz**, **CH09 2452MHz**, **CH10 2457MHz** or **CH11 2462MHz**.	**CH01 2412MHz**
RTS Threshold	RTS (Request To Send) threshold (number of bytes) enables RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC Service Data Unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432.	**2432**
Fragment Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.	**2432**
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

For WEP key configuration, refer to section on *WEP Data Encryption*.

3.11.3 Roaming

A wireless station is a computer with an IEEE 802.11b compliant wireless Network Interface Card (NIC). An Access Point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access point’s coverage area.

In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending on the signal strength, network utilization or other factors.

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the

signal of a new access point, which then informs the access points on the LAN about the change. The new information is then propagated to the other access points on the LAN. An example is shown in *Figure 3-10.*

If the roaming feature is not enabled on the access points, information is not communicated between the access points when a wireless station moves between coverage areas. The wireless station may not be able to communicate with other wireless stations on the network and vice versa.

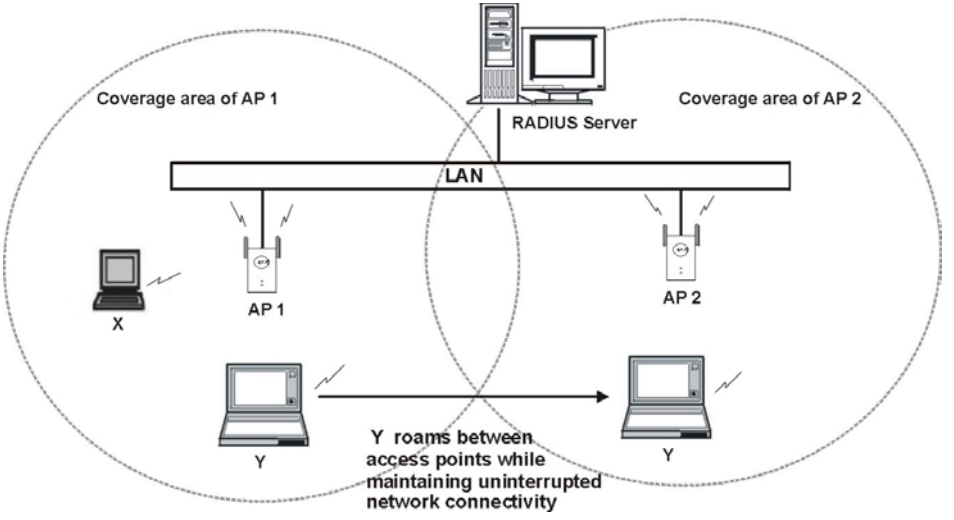

Figure 3-10 Roaming Example

The steps below describe the roaming process.

Step 1. As wireless station **Y** moves from the coverage area of access point **AP 1** to that of acces point **AP 2**, it scans and uses the signal of access point **AP 2**.

Step 2. Access point **AP 2** acknowledges the pressence of wireless station **Y** and relays this information to access point **AP 1** through the wired LAN.

Step 3. Access point **AP 1** updates the new position of wireless station **.**

Step 4. Wireless station **Y** sends a request to access point **AP 2** for reauthentication.

3.11.4 Requirements for Roaming

The following requirements must be met in order for wireless stations to roam between the coverage areas.

1. All the access points must be on the same subnet and configured with the same ESSID.
2. If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.

3. The adjacent access points should use different radio channels when their coverage areas overlap.
4. All access points must use the same port number to relay roaming information.
5. The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

3.11.5 Enable the Roaming Feature on the ZyAIR

Enable the roaming feature if you have two or more ZyAIRs on the same subnet. Follow the steps below to allow roaming on your ZyAIR.

Step 1. From the main menu, enter 3 to display **Menu 3 – LAN Setup**.

Step 2. Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.

```
                Menu 3.5 - Wireless LAN Setup

ESSID= Wireless
Hide ESSID= No
Channel ID= CH01 2412MHz
RTS Threshold= 2432
Frag. Threshold= 2432
WEP= Disable
  Default Key= N/A
  Key1= N/A
  Key2= N/A
  Key3= N/A
  Key4= N/A
Edit MAC Address Filter= No
Edit Roaming Configuration= Yes


Press ENTER to Confirm or ESC to Cancel:
```

Figure 3-11 Wireless LAN Setup

Step 3. Move the cursor to the **Edit Roaming Configuration** field. Press [SPACE BAR] to select **Yes** and then press [ENTER]. **Menu 3.5.2 – Roaming Configuration** displays as shown next.

```
          Menu 3.5.2 - Roaming Configuration

        Active= Yes
        Port #= 16290


       Press ENTER to Confirm or ESC to Cancel:
```

Figure 3-12 Menu 3.5.2 – Roaming Configuration

The following table describes the fields in this menu.

Table 3-7 Roaming Configuration Field Descriptions

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to allow roaming on the ZyAIR Press [SPACE BAR] and then [ENTER] to select **Yes** to enable roaming on the ZyAIR if you have two or more ZyAIRs on the same subnet..
Port #	Enter the port number to communicate roaming information between access points. The port number must be the same on all access points. The default is **16290**. Make sure this port is not used by other services.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Part II:

ADVANCED APPLICATIONS

This part shows how to configure Wireless Security, Remote Node, Remote Node TCP/IP and NAT.

Chapter 4
Wireless LAN Security Setup

This chapter describes the types of security you can enable on the ZyAIR.

4.1 Levels of Security

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and other wireless.

The figure below shows the possible wireless security levels on your ZyAIR. The highest security level is EAP (Extensible Authentication Protocol) authentication. It requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or your LAN to provide authentication service for wireless clients.

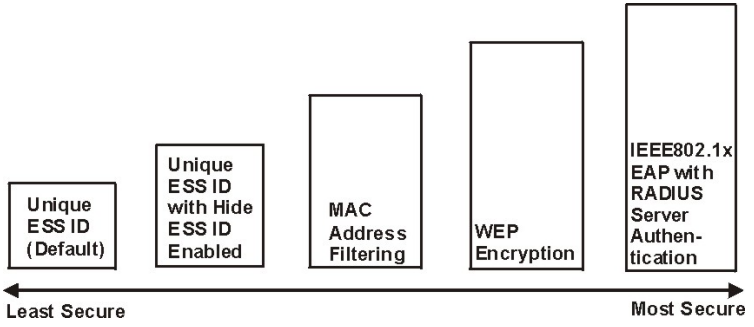

Figure 4-1 ZyAIR Wireless Security Levels

If you do not enable any wireless security on your ZyAIR, your network is accessible to any wireless networking device that is within range.

4.2 Data Encryption with WEP

WEP encryption scrambles the data transmitted between the wireless clients and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless clients and the access points must use the same WEP key for data encryption and decryption. For wireless LAN setup, refer to section on *Wireless LAN Setup***.**

Your ZyAIR allows you to configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time. Follow the steps below to configure and enable WEP encryption.

Step 1. From the main menu, enter 3 to display **Menu 3 – Lan Setup**.

Step 2. Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.

```
                Menu 3.5 - Wireless LAN Setup

ESSID= 432545
Hide ESSID= No
Channel ID= CH11 2462MHz
RTS Threshold= 2432
Frag. Threshold= 2432
WEP= Disable
  Default Key= N/A
  Key1= N/A
  Key2= N/A
  Key3= N/A
  Key4= N/A
Edit MAC Address Filter= No
Edit Roaming Configuration= No
```

Figure 4-2 Wireless LAN Setup

The following table describes the WEP related fields in this screen. For wireless LAN field descriptions refer to section on *Wireless LAN Setup*.

Table 4-1 Wireless LAN Setup Field Description

FIELD	DESCRIPTION	EXMAPLE
WEP	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select **Disable** to allow wireless clients to communicate with the access points without any data encryption. Select **64-bit WEP** or **128-bit WEP** to enable data encryption.	**Disable**
Default Key	Enter the key number (1 to 4) in this field. Only one key cab be enabled at any one time.	1
Key 1 to Key 4	If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 hexadecimal digits ("0-9", "A-F") preceded by 0x for each key. If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal digits ("0-9", "A-F") preceded by 0x for each key. There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless client computers.	
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

4.3 Network Authentication

Before a wireless client can communicate on your network through your ZyAIR, it must be authenticated by the ZyAIR or your network.

4.3.1 EAP

EAP is an authentication protocol designed originally to run over PPP (Point-to-Point Protocol) frame in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless client and a RADIUS server to perform mutual authentication.

4.3.2 RADIUS

RADIUS is based on a client-sever model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- **Authentication**

  Determines the identity of the users.

- **Authorization**

  Determines the network services available to authenticated users once they are connected to the network.

- **Accounting**

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your ZyAIR acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- **Access-Request**

  Sent by an access point requesting authentication.

- **Access-Reject**

  Sent by a RADIUS server rejecting access.

- **Access-Accept**

  Sent by a RADIUS server allowing access.

- **Access-Challenge**

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- **Accounting-Request**

  Sent by the access point requesting accounting.

- **Accounting-Response**

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

4.3.3 Sequence for EAP Authentication

The following figure shows the authentication steps when you enable EAP and specify a RADIUS server on your access point.

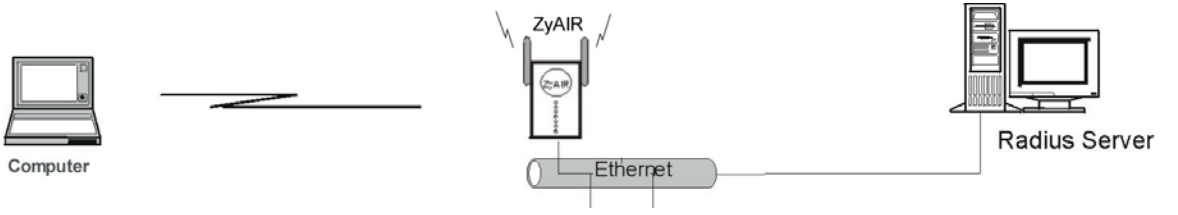

Figure 4-3 Sequence for EAP Authentication

The steps below describe how the IEEE 802.1X EAP authentication works.

Step 1. The wireless client sends a “request” message to the ZyAIR..

Step 2. The ZyAIR sends a “request” message to the wireless client for identity information.

Step 3. The wireless client replies with the password and username information.

Step 4. The ZyAIR receives the message and repackets this information into an Access-Request package which is then sent to the remote RADIUS server (or the Authentication server).

Step 5. The RADIUS server checks the user information against its user profile database and sends an "accept" or a "deny" packet to ZyAIR.

Step 6. When ZyAIR receives the "accept" package, the client port is placed into an authorized state and traffic is allowed to proceed. Otherwise, no traffic is allowed.

4.3.4 Enable EAP Authentication on Your ZyAIR

Follow the steps below to enable EAP authentication on your ZyAIR.

Step 1. From the main menu, enter 23 to display **Menu23 – System Security**.

```
Menu 23 - System Security

 1. Change Password
 2. RADIUS Server

 4. IEEE802.1X
```

Figure 4-4 Menu 23 – System Security

Step 2. Enter 4 to display **Menu 23.4 – System Security – IEEE802.1X**.

```
Menu 23.4 - System Security - IEEE802.1X

Authentication Control= Force Authorized
ReAuthentication Timer (in second)= N/A

Press ENTER to Confirm or ESC to Cancel:
```

Figure 4-5 Menu 23.4- System Security – IEEE802.1X

The following table describes the fields in this screen.

Table 4-2 IEEE802.1X System Security Field Descriptions

FIELD	DESCRIPTION
Authentication Control	Press [SPACE BAR] to select from **Forced Authorized**, **Forced Unauthorized** or **Auto**. The default is **Forced Authorized**. Select **Auto** to authenticate all wireless clients. Select **Force Authorized** to allow any user access to your wireless network without authentication. Select **Force UnAuthorized** to deny all user access to your wireless network.

Table 4-2 IEEE802.1X System Security Field Descriptions

FIELD	DESCRIPTION
ReAuthentication Timer (in seconds)	Specify the time interval between the RADIUS server's authentication checks of wireless users connected to the network. This field is activated only when you select **Auto** authentication control. The default time interval is **1800** seconds.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Once you enable the EAP authentication, you need to specify the external RADIUS server or create local user accounts for authentication.

4.3.5 Configuring External RADIUS Server

From **Menu 23- System Security**, enter 2 to display **Menu 23.2 - System Security-RADIUS Server** as shown next.

```
Menu 23.2 - System Security - RADIUS Server

                Authentication Server:
                  Active= No
                  Server Address= ?
                  Port #= 1812
                  Key= ?

                Accounting Server:
                  Active= No
                  Server Address= ?
                  Port #= 1813
                  Key= ?
```

Figure 4-6 Menu 23.2 System Security - External Server

The following table describes the fields in this screen.

Table 4-3 Menu 23.2 System Security - External Server Field Description

FIELD	DESCRIPTION	EXAMPLE
Authentication Server		
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external authentication server. Select **No** to enable user authentication using the local user profile on the ZyAIR.	**No**

Table 4-3 Menu 23.2 System Security - External Server Field Description

FIELD	DESCRIPTION	EXAMPLE
Server Address	Enter the IP address of the external authentication server in dotted decimal notation.	10.11.12.13
Port	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.	**1812**
Key	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points. The key is not sent over the network. This key must be the same on the external authentication server and ZyAIR.	
Accounting Server		
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external accounting server.	**No**
Server Address	Enter the IP address of the external accounting server in dotted decimal notation.	10.11.12.13
Port	The default port of the RADIUS server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.	**1813**
Key	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points. The key is not sent over the network. This key must be the same on the external accounting server and ZyAIR.	
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

4.4 Creating User Accounts on the ZyAIR

By storing user profiles locally, your ZyAIR is able to authenticate wireless users without interacting with a network RADIUS server.

Follow the steps below to set up user profiles on your ZyAIR.

Step 1. From the main menu, enter 14 to display **Menu 14 - Dial-in User Setup**.

```
                    Menu 14 - Dial-in User Setup

   1. ________      9. ________      17. ________      25. ________
   2. ________      10. ________     18. ________      26. ________
   3. ________      11. ________     19. ________      27. ________
   4. ________      12. ________     20. ________      28. ________
   5. ________      13. ________     21. ________      29. ________
   6. ________      14. ________     22. ________      30. ________
   7. ________      15. ________     23. ________      31. ________
   8. ________      16. ________     24. ________      32. ________

                        Enter Menu Selection Number:
```

Figure 4-7 Menu 14- Dial-in User Setup

Step 2. Type a number and press [ENTER] to edit the user profile.

```
                     Menu 14.1 - Edit Dial-in User

                    User Name= test
                    Active= Yes
                    Password= ********

                    Press ENTER to Confirm or ESC to Cancel:
```

Figure 4-8 Menu 14.1- Edit Dial-in User

The following table describes the fields in this screen.

Table 4-4 Menu 14.1- Edit Dial-in User Field Description

FIELD	DESCRIPTION
User Name	Enter a username up to 31 alphanumeric characters long for this user profile.
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable the user profile.
Password	Enter a password up to 31 characters long for this user profile.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

4.5 MAC Address Filtering

Your ZyAIR checks the MAC address of the wireless client device against a list of allowed or denied MAC addresses. However, intruders could fake allowed MAC addresses so MAC-based authentication is less secure than EAP authentication.

Follow the steps below to create the MAC address table on your ZyAIR.

Step 1. From the main menu, enter 3 to open **Menu 3 – LAN Setup**.

Step 2. Enter 5 to display **Menu 3.5 – Wireless LAN Setup**.

```
                Menu 3.5 - Wireless LAN Setup

                   ESSID= 432545
                   Hide ESSID= No
                   Channel ID= CH11 2462MHz
                   RTS Threshold= 2432
                   Frag. Threshold= 2432
                   WEP= Disable
                     Default Key= N/A
                     Key1= N/A
                     Key2= N/A
                     Key3= N/A
                     Key4= N/A
                   Edit MAC Address Filter= No
                   Edit Roaming Configuration= No

            Press ENTER to Confirm or ESC to Cancel:
```

Figure 4-9 Menu 3.5 – Wireless LAN Setup

Step 3. In the **Edit MAC Address Filtering** field, press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 3.5.1 – WLAN MAC Address Filter** displays as shown next.

```
                  Menu 3.5.1 - WLAN MAC Address Filter

                Active= No
                Filter Action= Allowed Association
                MAC Address Filter
                  Address  1= 00:00:00:00:00:00
                  Address  2= 00:00:00:00:00:00
                  Address  3= 00:00:00:00:00:00
                  Address  4= 00:00:00:00:00:00
                  Address  5= 00:00:00:00:00:00
                  Address  6= 00:00:00:00:00:00
                  Address  7= 00:00:00:00:00:00
                  Address  8= 00:00:00:00:00:00
                  Address  9= 00:00:00:00:00:00
                  Address 10= 00:00:00:00:00:00
                  Address 11= 00:00:00:00:00:00
                  Address 12= 00:00:00:00:00:00

                 Enter here to CONFIRM or ESC to CANCEL:
```

Figure 4-10 Menu 3.5.1 – WLAN MAC Address Filter

The following table describes the fields in this menu.

Table 4-5 MAC Address Filter Field Description

FIELD	DESCRIPTION
Active	To enable MAC address filtering, press [SPACE BAR] to select **Yes** and press [ENTER].
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. To deny access to the ZyAIR, press [SPACE BAR] to select **Deny Association** and press [ENTER]. MAC addresses not listed will be allowed to access the router. The default action, **Allowed Association**, permits association with the ZyAIR. MAC addresses not listed will be denied access to the router.
MAC Address Filter	
Address 1..12	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the client computers that are allowed or denied access to the ZyAIR in these address fields.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Chapter 5
Remote Node Configuration

This chapter shows you how to set up remote nodes on the WAN side.

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. When you use menu 4 to set up Internet access, you are configuring one of the remote nodes.

5.1 Remote Node Profile

Use **Menu 11-Remote Node Profile** to setup the remote node.

From the main menu, enter 11 to display **Menu 11-Remote Node Profile** as shown in *Figure 5-1*.

5.1.1 Encapsulation Scenarios

For Internet access you should use the encapsulation used by your ISP.

Nailed-Up Connection (PPPoE/PPTP)

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The ZyAIR does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the ZyAIR will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

```
                    Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe              Route= IP
Active= Yes

Encapsulation= PPTP                  Edit IP= No
Service Type= Standard               Telco Option:
Service Name= N/A                      Allocated Budget(min)= 0
Outgoing:                              Period(hr)= 0
  My Login=                            Schedules=
  My Password= ********                Nailed-Up Connection= No
  Authen= CHAP/PAP
PPTP:                                Session Options:
  My IP Addr=                          Edit Filter Sets= No
  My IP Mask=                          Idle Timeout(sec)= 100
  Server IP Addr=
  Connection ID/Name=

               Press ENTER to Confirm or ESC to Cancel:
```

Figure 5-1 Menu 11.1 - Remote Node Profile

In **Menu 11.1 – Remote Node Profile**, fill in the fields as described in the following table.

Table 5-1 Remote Node Profile Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Type a unique, descriptive name of up to eight characters for this node.	ChangeMe
Active	Press [SPACE BAR] and then [ENTER] to select **No** to deactivate this node. Inactive nodes are displayed with a minus sign "–" in SMT menu 11.	**Yes** (default)
Encapsulation	Press [SPACE BAR] to select from **Ethernet**, **PPPoE** or **PPTP** and press [ENTER].	Ethernet
Service Type	Press [SPACE BAR] and then [ENTER] to select the service type. Choose a RoadRunner flavor if your ISP is using Time Warner's RoadRunner; otherwise choose **Standard**. The User Name, Password and Login Server IP Address fields are not applicable (N/A) for the latter. Choose from **Standard**, **Telstra** (RoadRunner Telstra or BigPond authentication method), **RR-Manager** (RoadRunner Manager authentication method) or **RR-Toshiba** (RoadRunner Toshiba authentication method).	Standard
Service Name	When using **PPPoE** encapsulation, type the name of your PPPoE service here.	N/A

Table 5-1 Remote Node Profile Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Outgoing: My Login	Type the login name assigned by your ISP when the ZyAIR calls this remote node.	
My Password	Type the password assigned by your ISP when the ZyAIR calls this remote node.	
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP**/**PAP** – Your ZyAIR will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** – accept **CHAP** (Challenge Handshake Authentication Protocol) only. **PAP** – accept PAP (Password Authentication Protocol) only.	**PAP**
PPTP:		
My IP Address	Type the (static) IP address assigned to you by your ISP in dotted decimal notation.	10.11.12.13
My IP Mask	Type the subnet mask of the PPTP server.	
Server IP Address	Type the IP address of the PPTP server in dotted decimal notation.	
Connection ID/Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your xDSL modem.	
Route	This field determines the protocol used in routing. Options are **IP** and **None.**	**IP** (default)
Edit IP	Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options**.	**No**
Telco Option:	**Telco Option** is available only for PPTP or PPPoE encapsulation.	
Allocated Budget (min)	This sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.	0 (default)

Table 5-1 Remote Node Profile Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Period (hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the **Allocated Budget** is (10 minutes) and the **Period (hr)** is 1 (hour).	0 (default)
Schedule	This field is only applicable for **PPPoE** and **PPPTP** encapsulation. You can apply up to four schedule sets here. For more details please refer to the *Call Schedule Setup* chapter.	
Nailed up Connection	This field is only applicable for **PPPoE** and **PPTP** encapsulation. This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.	
Session Options Edit Filter Sets	Use [SPACE BAR] to choose **Yes** and press [ENTER] to open menu 11.5 to edit the filter sets. See the *Remote Node Filter* section for more details.	**No** (default)
Idle Timeout (sec)	Type the number of seconds (0-9999) that can elapse when the ZyAIR is idle (there is no traffic going to the remote node), before the ZyAIR automatically disconnects the remote node. 0 means that the session will not timeout. This field is available only for PPTP or PPPoE encapsulations.	100 (default)
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

5.1.2 Outgoing Authentication Protocol

For obvious reasons, you should employ the strongest authentication protocol possible. However, some vendors’ implementation includes specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If the peer disconnects right after a successful authentication, make sure that you specify the correct authentication protocol when connecting to such an implementation.

5.1.3 Remote Node Setup

For the TCP/IP parameters, perform the following steps to edit **Menu 11.3 - Remote Node Network Layer Options**.

Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes,** then press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options** shown below.

```
Menu 11.3 - Remote Node Network Layer Options

  IP Address Assignment= Static
  Rem IP Addr= 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0

  Network Address Translation= None
  Metric= 1
  Private= No
  RIP Direction= None
    Version= N/A
  Multicast= None


   Enter here to CONFIRM or ESC to CANCEL:
```

Figure 5-2 Remote Node Network Layer Options

The next table explains fields in **Menu 11.3 - Remote Node Network Layer Options**.

Table 5-2 Remote Node Network Layer Options

FIELD	DESCRIPTITON	EXAMPLE
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select **Dynamic** if the remote node is using a dynamically assigned IP address or **Static** if it is using a static (fixed) IP address. You will only be able to configure this in the ISP node (also the one you configure in menu 4), all other nodes are set to **Static**.	**Static**
Rem IP Addr	This is the IP address you entered in the previous menu.	
Rem Subnet Mask	Type the subnet mask assigned to the remote node.	
My WAN Addr	Some implementations, especially UNIX derivatives, require separate IP network numbers for the WAN and LAN links and each end to have a unique address within the WAN network number. In that case, type the IP address assigned to the WAN port of your ZyAIR.	
Network Address Translation	Press [SPACE BAR] and then [ENTER] to select **Full Feature** if you have multiple public WAN IP addresses for your ZyAIR.	**Full Feature**

Table 5-2 Remote Node Network Layer Options

FIELD	DESCRIPTITON	EXAMPLE
	Select **SUA Only** if you have just one public WAN IP address for your ZyAIR. The SMT uses Address Mapping Set 255 (menu 15.1 - see section *6.3.1*). Select **None** to disable NAT.	
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the cost measurement, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	2
Private	This determines if the ZyAIR will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.	**No**
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP Direction. Options are **Both**, **In Only**, **Out Only** or **None**.	**None**
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1**
Multicast	**IGMP-v1** sets IGMP to version 1, **IGMP-v2** sets IGMP to version 2 and **None** disables IGMP.	**None**
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

5.2 Remote Node Filter

Move the cursor to the **Edit Filter Sets** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to display **Menu 11.5 - Remote Node Filter**.

Use **Menu 11.5 - Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ZyAIR and also to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by comma, for example, 1, 5, 9, 12, in each filter field.

Note that spaces are accepted in this field.

```
                    Menu 11.5 - Remote Node Filter

                         Input Filter Sets:
                           protocol filters= 1, 2, 3
                             device filters=
                        Output Filter Sets:
                           protocol filters=
                             device filters=

          Enter here to CONFIRM or ESC to CANCEL:
```

Figure 5-3 Menu 11.5 - Remote Node Filter (Ethernet Encapsulation)

```
                Menu 11.5 - Remote Node Filter

                             Input Filter Sets:
                             protocol filters=
                              device filters=
                            Output Filter Sets:
                            protocol filters= 1
                              device filters=
                             Call Filter Sets:
                             protocol filters=
                              device filters=


           Enter here to CONFIRM or ESC to CANCEL:
```

Figure 5-4 Menu 11.5 - Remote Node Filter (PPTP or PPPoE Encapsulation)

5.2.1 IP Static Route Setup

Static routes tell the ZyAIR routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node.

Each remote node specifies only the network to which the gateway is directly connected and the ZyAIR has no knowledge of the networks beyond. For instance, the ZyAIR knows about network N2 in the following figure through remote node Router 1. However, the ZyAIR is unable to route a packet to network N3 because it does not know that there is a route through remote node Router 1 (via Router 2). The static routes allow you to tell the ZyAIR about the networks beyond the remote nodes.

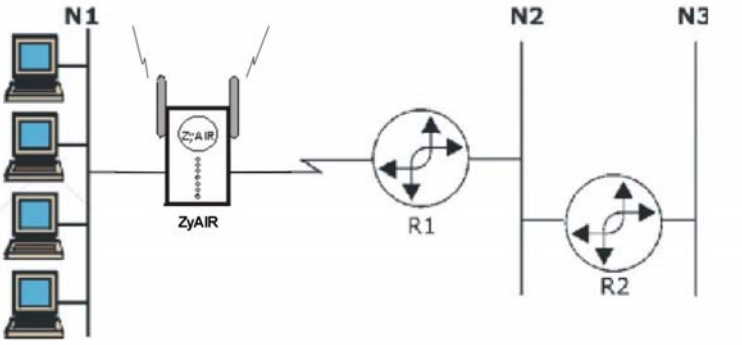

Figure 5-5 Sample Static Routing Topology

Configuration

Step 1. To configure an IP static route, use **Menu 12 - Static Route Setup** as shwon next.

```
                Menu 12 - IP Static Route Setup

                  1. ________
                  2. ________
                  3. ________
                  4. ________
                  5. ________
                  6. ________
                  7. ________
                  8. ________

                   Enter selection number:
```

Figure 5-6 Menu 12.1 - IP Static Route Setup

Step 2. Now, type the route number of a static route you want to configure.

```
                Menu 12.1 - Edit IP Static Route

              Route #: 1
              Route Name= ?
              Active= No
              Destination IP Address= ?
              IP Subnet Mask= ?
              Gateway IP Address= ?
              Metric= 2
              Private= No

            Press ENTER to Confirm or ESC to Cancel:
```

Figure 5-7 Edit IP Static Route

The following table describes the fields for **Menu 12.1 - Edit IP Static Route Setup**.

Table 5-3 Edit IP Static Route Menu Fields

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.1.
Route Name	Type a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Type the subnet mask for this destination. Follow the discussion on *IP Subnet Mask* in this manual.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyAIR that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyAIR; over WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the ZyAIR will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and is not included in RIP broadcasts. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.

Chapter 6
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the ZyAIR.

6.1 Introduction

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

6.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyAIR, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 6-1 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside **host.**

6.1.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. Although you can make designated servers on the LAN accessible to the outside world, it is strongly recommended that you attach those servers to the DMZ port instead. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see *Table 6-2*), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyAIR filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

6.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyAIR keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

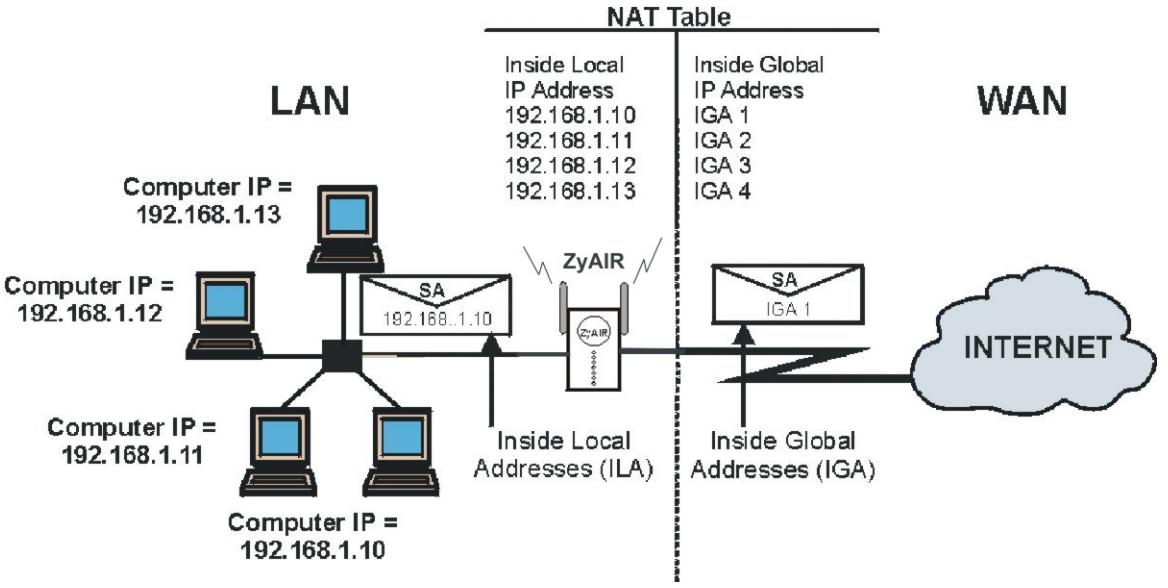

Figure 6-1 How NAT Works

6.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the ZyAIR can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

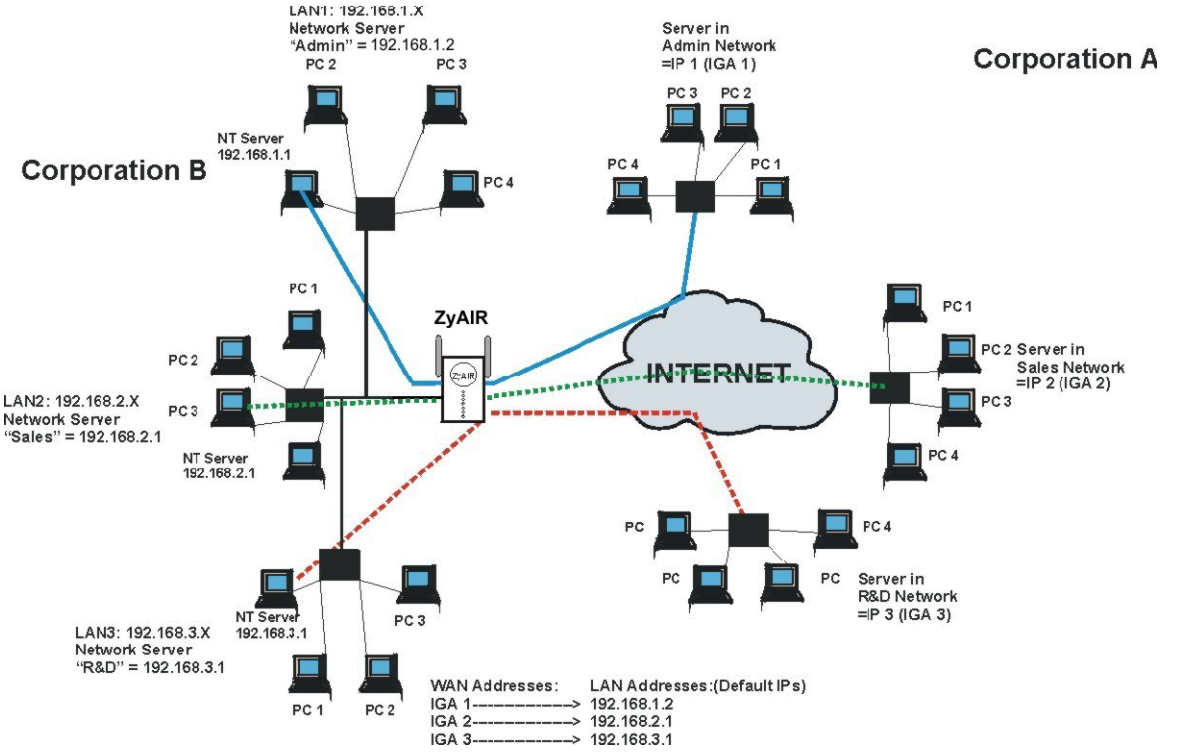

Figure 6-2 NAT Application With IP Alias

6.1.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

1. **One to One**: In One-to-One mode, the ZyAIR maps one local IP address to one global IP address.
2. **Many to One**: In Many-to-One mode, the ZyAIR maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for instance, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today's routers).
3. **Many to Many Overload**: In Many-to-Many Overload mode, the ZyAIR maps the multiple local IP addresses to shared global IP addresses.
4. **Many One-to-One**: In Many One-to-One mode, the ZyAIR maps each local IP address to a unique global IP address.

5. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world although, it is highly recommended that you use the DMZ port for these servers instead.

Port numbers do not **change for** One-to-One **and** Many One-to-One **NAT mapping types.**

The following table summarizes these types.

Table 6-2 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-One	ILA1←→ IGA1	1:1
Many-to-One (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 …	M:1
Many-to-Many Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 …	M:M Ov
Many One-to-One	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 …	M-1-1
Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1	Server

6.2 Using NAT

6.2.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See section *6.3.1* for a detailed description of the NAT set for SUA. The ZyAIR also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in *Table 6-2*.

1. **Choose** SUA Only **if you have just one public WAN IP address for your ZyAIR.**
2. **Choose** Full Feature **if you have multiple public WAN IP addresses for your ZyAIR.**

6.2.2 Applying NAT

You apply NAT via menus 4 or 11.3 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.

```
Menu 4 - Internet Access Setup

    ISP's Name= ChangeMe
    Encapsulation= Ethernet
      Service Type= Standard
      My Login= N/A
      My Password= N/A
      Login Server= N/A

    IP Address Assignment= Dynamic
      IP Address= N/A
      IP Subnet Mask= N/A
      Gateway IP Address= N/A
    Network Address Translation= Full Feature

Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-3 Menu 4 - Applying NAT for Internet Access

The following figure shows how you apply NAT to the remote node in menu 11.1.

Step 1. Enter 11 from the main menu.

Step 2. Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options.**

```
Menu 11.3 - Remote Node Network Layer Options

  IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Addr= N/A

  Network Address Translation= Full Feature
  Metric= 1
  Private= N/A
  RIP Direction= None
    Version= N/A
  Multicast= None


  Enter here to CONFIRM or ESC to CANCEL:
```

Figure 6-4 Menu 11.3 - Applying NAT to the Remote Node

The following table describes the options for Network Address Translation.

Table 6-3 Applying NAT in Menus 4 & 11.3

FIELD	DESCRIPTION	EXAMPLE
Network Address Mapping	Press [SPACE BAR] and then [ENTER] to select **Full Feature** if you have multiple public WAN IP addresses for your ZyAIR.	**Full Feature**
	Select **None** to disable NAT.	
	When you select **SUA Only**, the SMT uses Address Mapping Set 255 (menu 15.1 - see *Section 6.3.1*). Choose **SUA Only** if you have just one public WAN IP address for your ZyAIR.	

6.3 NAT Setup

Use the Address Mapping Sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. You can see two NAT Address Mapping sets in menu 15.1. You can only configure **Set 1**. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**, which supports all mapping types as outlined in *Table 6-2*. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The Server Set is a list of LAN side servers mapped to external ports. To use this set, a server rule must be set up inside the NAT Address Mapping set. Please see *Section 6.4* for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

```
                    Menu 15 - NAT Setup

          1.    Address Mapping Sets
          2.    NAT Server Sets


                     Enter Menu Selection Number:
```

Figure 6-5 Menu 15 - NAT Setup

6.3.1 Address Mapping Sets

Enter 1 to bring up **Menu 15.1 – Address Mapping Sets**.

```
                Menu 15.1 - Address Mapping Sets

                   1.
                 255. SUA (read only)


                  Enter Menu Selection Number:
```

Figure 6-6 Menu 15.1 - Address Mapping Sets

SUA Address Mapping Set

Enter 255 to display the next screen (see also *Section 6.2.1)*. The fields in this menu cannot be changed.

Menu 15.1.255 is read-only.

```
          Menu 15.1.1 - Address Mapping Rules

  Set Name= SUA

 Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
 ---  ---------------  ---------------  ---------------  ---------------  ------
  1.  0.0.0.0          255.255.255.255  0.0.0.0                           M-1
  2.                                    0.0.0.0                           Server
  3.
  4.
  5.
  6.
  7.
  8.
  9.
 10.
```

Figure 6-7 Menu 15.1.255 - SUA Address Mapping Rules

The following table explains the fields in this screen.

Table 6-4 SUA Address Mapping Rules

FIELD	DESCRIPTION	EXAMPLE
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.	SUA
Idx	This is the index or rule number.	1
Local Start IP Local End IP	**Local Start IP** is the starting local IP address (ILA) (see *Figure 6-1)*. **Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.	0.0.0.0 255.255.255.255
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**.	0.0.0.0
Global End IP	This is the ending global IP address (IGA).	
Type	These are the mapping types discussed above (see *Table 6-2*). **Server** allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.	Server
Once you have finished configuring a rule in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel.		

User-Defined Address Mapping Sets

Now let's look at option 1 in menu 15.1. Enter 1 to bring up this menu. We'll just look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the "?" in the **Set Name** field means that this is a required field and you must enter a name for the set.

```
                        Menu 15.1.1 - Address Mapping Rules

  Set Name= ?

 Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
 ---  ---------------  ---------------  ---------------  ---------------  ------
  1.
  2
  3.
  4.
  5.
  6.
  7.
  8.
  9.
 10.
                   Action= Edit          Select Rule=

                   Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-8 Menu 15.1.1 - First Set

The table below describes the fields for configuration in this screen.

Table 6-5 Fields in Menu 15.1.1

FIELD	DESRIPTION	EXAMPLE
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.	NAT_SET
Action	The default is **Edit**. **Edit** means you want to edit a selected rule (see following field). **Insert Before** means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected one will be advanced one rule. **None** disables the **Select Rule** item.	**Edit**
Select Rule	When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.	1

You must press [ENTER] **at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.**

An End IP address must be numerically greater than its corresponding IP Start address.

If the Set Name **field is left blank, the entire set will be deleted.**

6.3.2 Configuring Individual Rule

In **Menu 15.1.1-Address Mapping Rules**, select **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.

```
                Menu 15.1.1.1 Address Mapping Rule

                   Type= One-to-One

                   Local IP:
                     Start=
                     End  = N/A

                   Global IP:
                     Start=
                     End  = N/A


                 Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-9 Menu 15.1.1.1 - Editing/Configuring an Individual Rule in a Set

Table 6-6 Menu 15.1.1.1 - Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION	EXAMPLE
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in *Table 6-2.* **Server** allows you to specify multiple servers of different types behind NAT to this computer. See *Section 6.5.3* for an example.	**One-to-One**
Local IP	Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**.	
Start	This is the starting local IP address (ILA).	0.0.0.0
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types.	N/A

FIELD	DESCRIPTION	EXAMPLE
Global IP		
Start	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server**.	0.0.0.0
End	This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**.	N/A
Server Mapping Set	Only available when **Type** is set to **Server**. Type a number from 1 to 10 to choose a server set from menu 15.2.	
Once you have finished configuring a rule in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel.		

Ordering Your Rules

Ordering your rules is important because the ZyAIR applies the rules in the order that you specify. When a rule matches the current packet, the ZyAIR takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9.

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

6.4 NAT Server Sets – Port Forwarding

A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Use **Menu 15 - NAT Setup** to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

The most often used port numbers are shown in the following table. Please refer to *RFC 1700* for further information about port numbers. Please also refer to the included disk for more examples and details on NAT.

Table 6-7 Services & Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

6.4.1 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

Step 1. Enter 15 in the main menu to go to **Menu 15 - NAT Setup.**

Step 2. Enter 2 to display **Menu 15.2 - NAT Server Sets** as shown next.

```
                    Menu 15.2 - NAT Server Setup

 Rule    Start Port No.    End Port No.    IP Address
-------------------------------------------------------
   1.     Default           Default         0.0.0.0
   2.       0                 0             0.0.0.0
   3.       0                 0             0.0.0.0
   4.       0                 0             0.0.0.0
   5.       0                 0             0.0.0.0
   6.       0                 0             0.0.0.0
   7.       0                 0             0.0.0.0
   8.       0                 0             0.0.0.0
   9.       0                 0             0.0.0.0
  10.       0                 0             0.0.0.0
  11.       0                 0             0.0.0.0
  12.       1027              1027          RR Reserved

        Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-10 Menu 15.2 - NAT Server Setup

Step 3. Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.

Step 4. Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.

Step 5. Press [ENTER] at the "Press ENTER to confirm …" prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

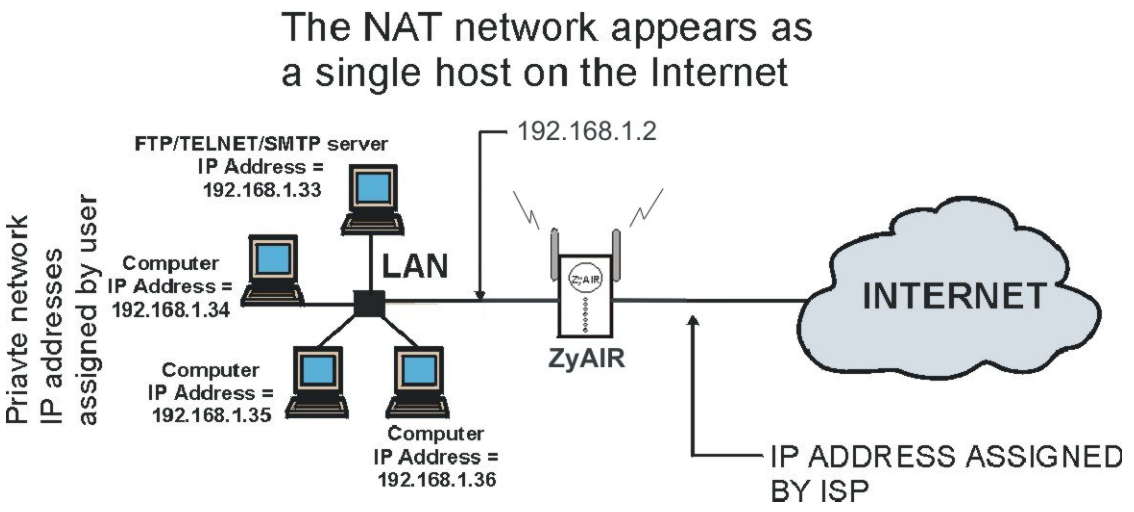

Figure 6-11 Multiple Servers Behind NAT Example

6.5 General NAT Examples

6.5.1 Example 1: Internet Access Only

In the following Internet access example, you only need one rule where your ILAs (Inside Local addresses) all map to one dynamic IGA (Inside Global Address) assigned by your ISP.

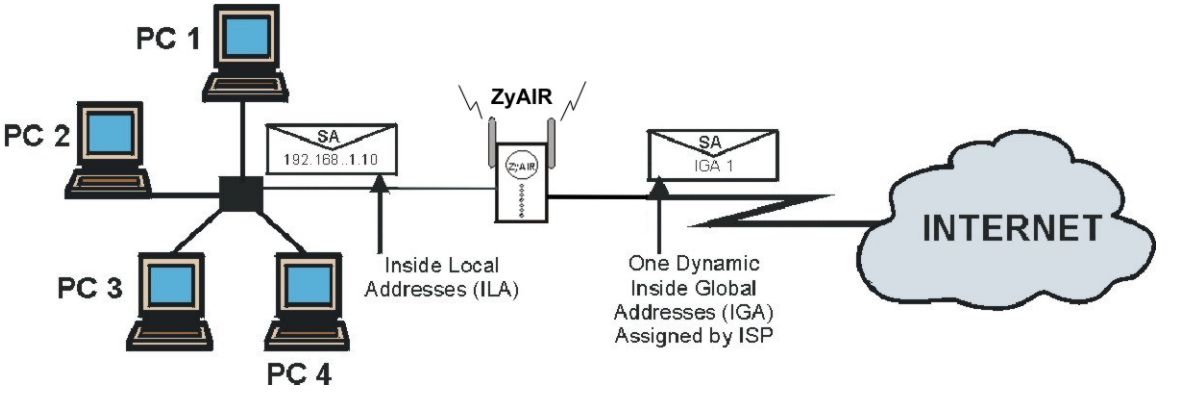

Figure 6-12 NAT Example 1

```
                Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= Ethernet
  Service Type= Standard
  My Login= N/A
  My Password= N/A
  Login Server= N/A

IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= SUA Only


Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-13 Menu 4 - Internet Access & NAT Example

From menu 4, choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section 6.5*. The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

6.5.2 Example 2: Internet Access with an Inside Server

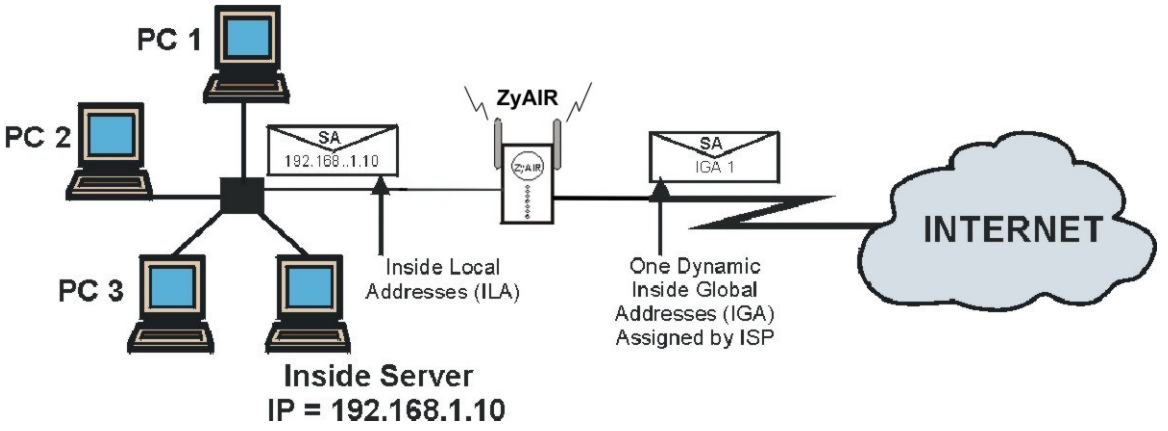

Figure 6-14 NAT Example 2

In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and then go to menu 15.2 to specify the Inside Server behind the NAT as shown in the next figure.

```
                    Menu 15.2 - NAT Server Setup

 Rule    Start Port No.    End Port No.    IP Address
-------------------------------------------------------
   1.    Default           Default         192.168.1.10
   2.      0                 0             0.0.0.0
   3.      0                 0             0.0.0.0
   4.      0                 0             0.0.0.0
   5.      0                 0             0.0.0.0
   6.      0                 0             0.0.0.0
   7.      0                 0             0.0.0.0
   8.      0                 0             0.0.0.0
   9.      0                 0             0.0.0.0
  10.      0                 0             0.0.0.0
  11.      0                 0             0.0.0.0
  12.      1027              1027          RR Reserved

        Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-15 Menu 15.2.1 - Specifying an Inside Server

6.5.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two uni-directional as follows.

Rule 1. Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

Rule 2. Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

Rule 3. Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

Rule 4. You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

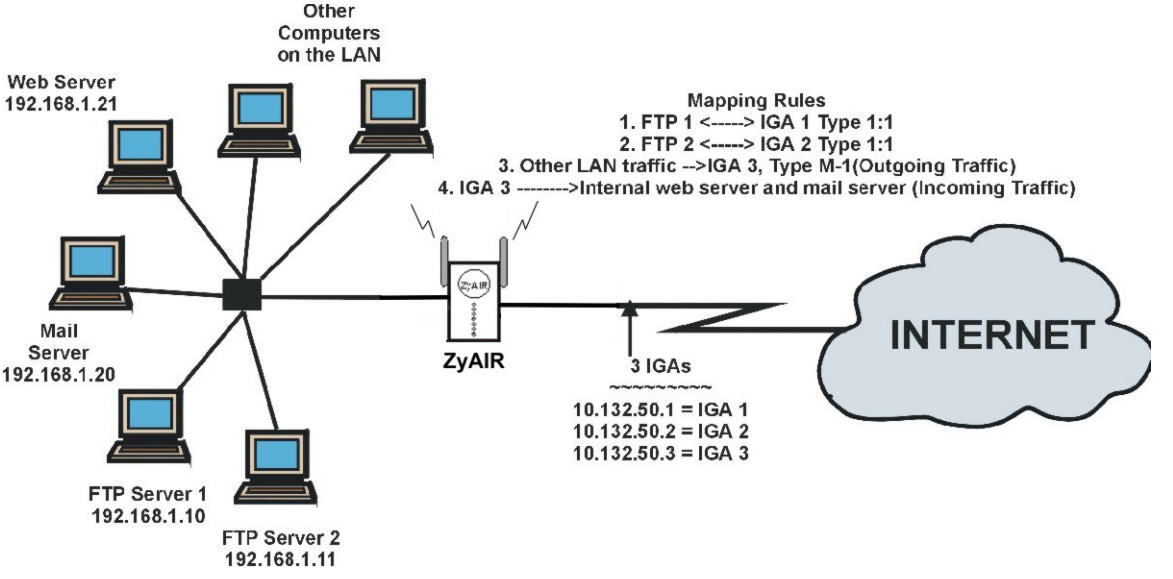

Figure 6-16 NAT Example 3

Step 1. In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets.** Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) as shown in the finger below.

```
Menu 11.3 - Remote Node Network Layer Options

   IP Address Assignment= Dynamic
   IP Address= N/A
   IP Subnet Mask= N/A
   Gateway IP Addr= N/A

   Network Address Translation= Full Feature
   Metric= 1
   Private= N/A
   RIP Direction= None
     Version= N/A
   Multicast= None

    Enter here to CONFIRM or ESC to CANCEL:
```

Figure 6-17 Example 3: Menu 11.3

Step 2. Then enter 15 from the main menu.

Step 3. Enter 1 to configure the Address Mapping Sets.

Step 4. Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.

Step 5. Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). The following figure shows how to configure the first rule

```
                Menu 15.1.1.1 Address Mapping Rule

              Type= One-to-One

              Local IP:
                Start= 192.168.1.10
                End  = N/A

              Global IP:
                Start= 10.132.50.1
                End  = N/A

             Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-18 Example 3: Menu 15.1.1.1

Step 6. Repeat the previous step for rules 2 to 4 as outlined above.

Step 7. When finished, menu 15.1.1 should look like as shown next.

```
                    Menu 15.1.1 - Address Mapping Rules

  Set Name= Eample3

 Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
 ---  ---------------  ---------------  ---------------  ---------------  ------
  1.  192.168.1.10                      10.132.50.1                       1-1
  2.  192.168.1.11                      10.132.50.2                       1-1
  3.  0.0.0.0          255.255.255.255  10.132.50.3                       M-1
  4.                                    10.132.50.3                       Server
  5.
  6.
  7.
  8.
  9.
 10.

                  Action= None          Select Rule= N/A

                  Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-19 Example 3: Final Menu 15.1.1

Now configure the IGA3 to map to our web server and mail server on the LAN.

Step 1. Enter 15 from the main menu.

Step 2. Enter 2 in to display **Menu 15.2 - NAT Server Sets** and configure it as shown.

```
                    Menu 15.2 - NAT Server Setup


          Rule   Start Port No.   End Port No.   IP Address
         ------------------------------------------------
            1.    Default          Default        0.0.0.0
            2.      80               80           192.168.1.21
            3.      25               25           192.168.1.20
            4.      0                0            0.0.0.0
            5.      0                0            0.0.0.0
            6.      0                0            0.0.0.0
            7.      0                0            0.0.0.0
            8.      0                0            0.0.0.0
            9.      0                0            0.0.0.0
           10.      0                0            0.0.0.0
           11.      0                0            0.0.0.0
           12.      1027             1027         RR Reserved

               Press ENTER to Confirm or ESC to Cancel:
```

Example 3: Menu 15.2

6.5.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many One-to-One** mapping as port numbers do *not* change for **Many One-to-One** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

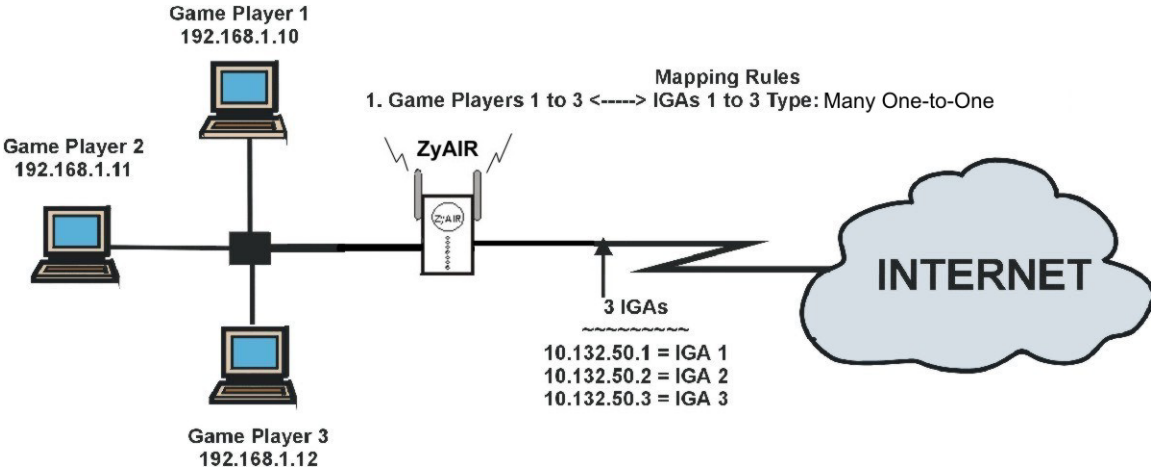

Figure 6-20 NAT Example 4

Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using One-to-One **and** Many One-to-One **mapping types.**

Follow the steps outlined in example 3 to configure these two menus as follows.

```
                    Menu 15.1.1.1 Address Mapping Rule

        Type= Many One-to-One

        Local IP:
          Start= 192.168.1.10
          End  = 192.168.1.12

        Global IP:
          Start= 10.132.50.1
          End  = 10.132.50.3

                    Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-21 Example 4: Menu 15.1.1.1

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

```
                        Menu 15.1.1 - Address Mapping Rules

 Set Name= Example4

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1.  192.168.1.10     192.168.1.12     10.132.50.1      10.132.50.3      M-1-1
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

                    Action= Edit          Select Rule=

                    Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-22 Example 4: Menu 15.1.1

Part III:

ADVANCED MANAGEMENT

This part discusses Filtering, SNMP, System Information and Diagnosis, Firmware and Configuration File Maintenance, System Maintenance and Information, IP Policy Routing, Call Scheduling and Remote Management.

Chapter 7
Filter Configuration

This chapter shows you how to create and apply filters.

7.1 About Filtering

Your ZyAIR uses filters to decide whether or not to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the Ethernet side. Call filtering is used to determine if a packet should be allowed to trigger a call.

Outgoing packets must undergo data filtering before they encounter call filtering. Call filters are divided into two groups, the built-in call filters and user-defined call filters. Your ZyAIR has built-in call filters that prevent administrative, for example, RIP packets from triggering calls. These filters are always enabled and not accessible to you. Your ZyAIR applies the built-in filters first and then the user-defined call filters, if applicable, as shown next.

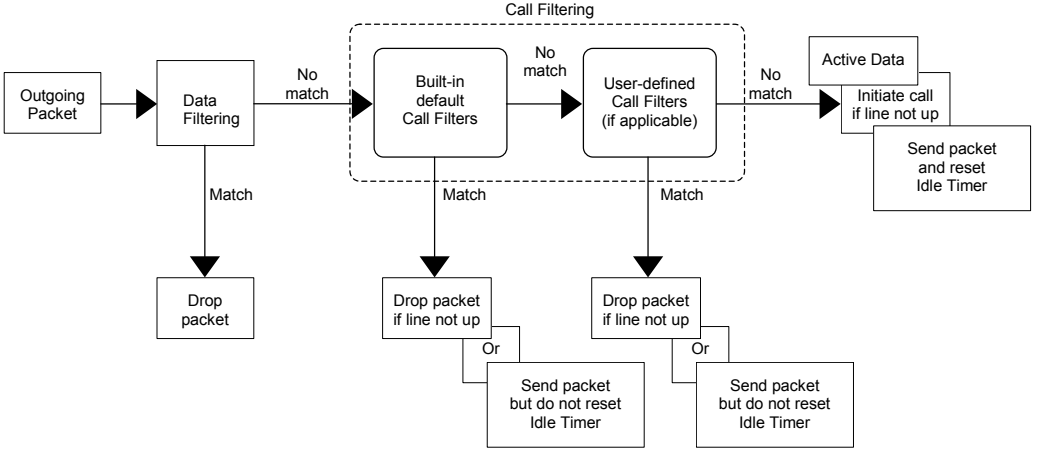

Figure 7-1 Outgoing Packet Filtering Process

Two sets of factory filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule.

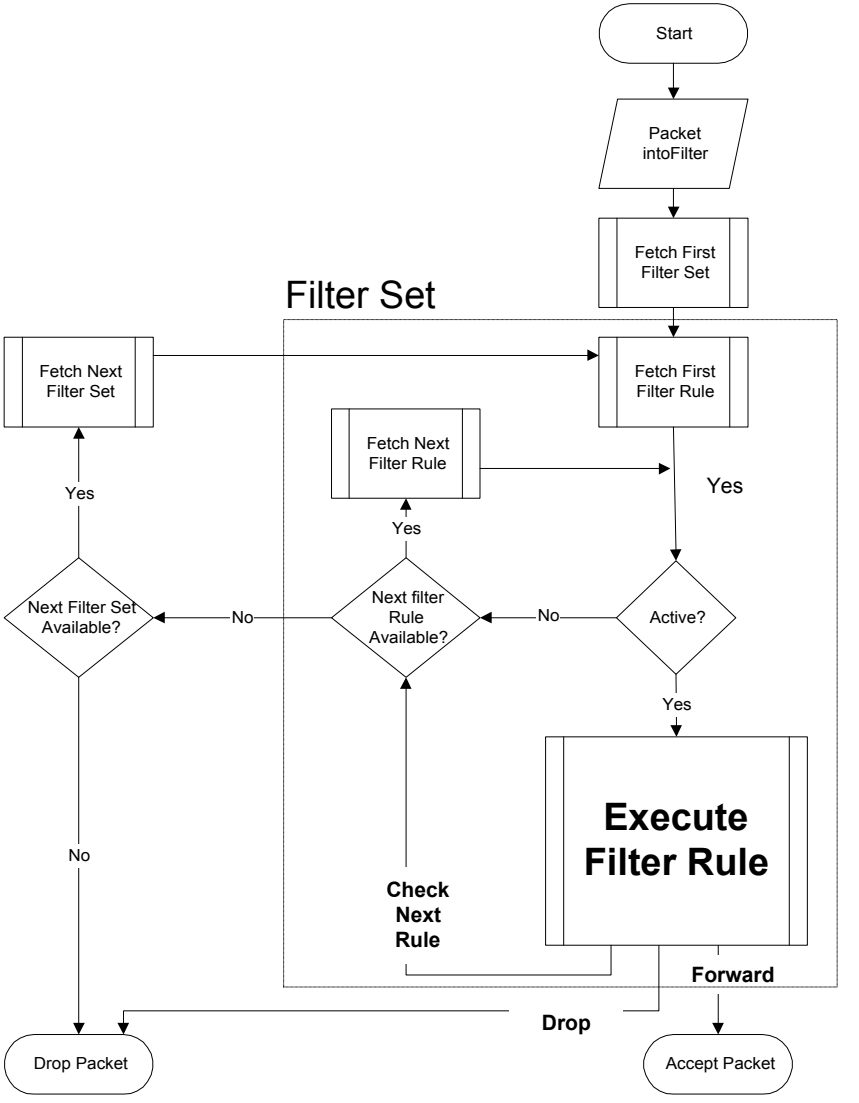

Figure 7-2 Filter Rule Process

You can apply up to four filter sets to a particular port to block various types of packets. Because each filter set can have up to six rules, you can have a maximum of 24 rules active for a single port.

For incoming packets, your ZyAIR applies data filters only. Packets are processed depending on whether a match is found. The following sections describe how to configure filter sets.

The Filter Structure of the ZyAIR

A filter set consists of one or more filter rules. Usually, you would group related rules, for example, all the rules for NetBIOS, into a single set and give it a descriptive name. You can configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.

7.2 Configuring a Filter Set

To configure a filter set, follow the steps shown next.

Step 1. Enter 21 in the main menu to display **Menu 21 – Filter Set Configuration**.

```
          Menu 21 - Filter Set Configuration

Filter                                Filter
Set #        Comments                 Set #        Comments
------  -----------------             ------  -----------------
  1      NetBIOS_WAN                     7      _______________
  2      NetBIOS_LAN                     8      _______________
  3      TEL_FTP_WEB_WAN                 9      _______________
  4      _______________                10      _______________
  5      _______________                11      _______________
  6      _______________                12      _______________



                Enter Filter Set Number to Configure= 0
```

Figure 7-3 Menu 21 – Filter Set Configuration

Step 2. Type the filter set to configure (no. 1 to 12) and press [ENTER].

Step 3. Type a descriptive name or comment in the **Comments** field and press [ENTER].

Step 4. Press [ENTER] at the message "Press ENTER to confirm…" to display **Menu 21.1 – Filter Rules Summary** (that is, if you selected filter set 1 in menu 21).

The following figures show the summary of three filter sets of your ZyAIR.

```
                    Menu 21.1 - Filter Rules Summary

# A Type                        Filter Rules                              M m n
- - ---- ------------------------------------------------------------------ - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137                              N D N
2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138                              N D N
3 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139                              N D N
4 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137                             N D N
5 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138                             N D N
6 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139                             N D F


                  Enter Filter Rule Number (1-6) to Configure:
```

Figure 7-4 NetBIOS_WAN Filter Rules Summary

```
                        Menu 21.2 - Filter Rules Summary

# A Type                        Filter Rules                              M m n
- - ---- ------------------------------------------------------------------ - - -
1 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53                      N D F
2 N
3 N
4 N
5 N
6 N


                  Enter Filter Rule Number (1-6) to Configure:
```

Figure 7-5 NetBIOS_LAN Filter Rules Summary

```
                        Menu 21.3 - Filter Rules Summary

# A Type                        Filter Rules                              M m n
- - ---- ------------------------------------------------------------------ - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23                               N D N
2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21                               N D N
3 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=80                               N D F
4 N
5 N
6 N


                  Enter Filter Rule Number (1-6) to Configure:
```

Figure 7-6 TEL_FTP_WEB_WAN Filter Rules Summary

7.2.1 Filter Rules Summary Menus

The following tables briefly describe the abbreviations used in menus 21.1 and 21.2.

Table 7-1 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
#	The filter rule number: 1 to 6.
A	Active: “Y” means the rule is active. “N” means the rule is inactive.
Type	The type of filter rule: “GEN” for Generic, “IP” for TCP/IP.
Filter Rules	These parameters are displayed here.
M	More. “Y” means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. “N” means there are no more rules to check. You can specify an action to be taken for instance, forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N“ means to check the next rule.
n	Action Not Matched. “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N” means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

Table 7-2 Rule Abbreviations Used

FILTER TYPE	DESCRIPTION
IP	
Pr	Protocol
SA	Source Address
SP	Source Port Number
DA	Destination Address
DP	Destination Port Number

Table 7-2 Rule Abbreviations Used

FILTER TYPE	DESCRIPTION
GEN	
Off	Offset
Len	Length

7.3 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1 – Filter Rules Summary** and press [ENTER] to open menu 21.1.1 for the rule.

There are two types of filter rules: **TCP/IP** and **Generic**. Depending on the type of rule, the parameters for each type will be different. Use [SPACE BAR] to select the type of rule that you want to create in the **Filter Type** field and press [ENTER] to open the respective menu.

To speed up filtering, all rules in a filter set must be of the same class, for instance, protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filters field or vice versa, the ZyAIR will warn you and will not allow you to save.

7.3.1 TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select TCP/IP Filter Rule from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1 – TCP/IP Filter Rule**, as shown next.

```
                Menu 21.1.1 - TCP/IP Filter Rule

          Filter #: 1,1
          Filter Type= TCP/IP Filter Rule
          Active= Yes
          IP Protocol= 6     IP Source Route= No
          Destination: IP Addr= 0.0.0.0
                       IP Mask= 0.0.0.0
                       Port #= 137
                       Port # Comp= Equal
               Source: IP Addr= 0.0.0.0
                       IP Mask= 0.0.0.0
                       Port #=
                       Port # Comp= None
          TCP Estab= No
          More= No           Log= None
          Action Matched= Drop
          Action Not Matched= Check Next Rule

          Press ENTER to Confirm or ESC to Cancel:
```

Figure 7-7 Menu 21.1.1 – TCP/IP Filter Rule

The following table describes how to configure your TCP/IP filter rule.

Table 7-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third filter rule of that set.	1,1
Filter Type	Press [SPACE BAR] and the [ENTER] to select filter type. Choices are **TCP/IP Filter Rule** or **Generic Filter Rule**.	**TCP/IP Filter Rule** (default)
Active	Select **Yes** to activate or **No** to deactivate the filter rule.	**No** (default)
IP Protocol	This is the upper layer protocol, for example, TCP is 6, UDP is 17 and ICMP is 1. The value must be between 0 and 255. A value of 0 matches ANY protocol.	0 to 255

Table 7-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	EXAMPLE
IP Source Route	IP Source Route is an optional header that dictates the route an IP packet takes from its source to its destination. If **Yes**, the rule applies to any packet with an IP source route. The majority of IP packets do not have source route.	**No** (default)
Destination: IP Addr	Type the destination IP address of the packet you want to filter. This field is ignored if it is 0.0.0.0.	IP address
IP Mask	Type the IP mask to apply to the Destination: IP Addr field.	IP mask
Port #	Type the destination port of the packets you want to filter. The field range is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in **Destination: Port #.** Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**.	**None**
Source: IP Addr	Type the source IP Address of the packet you want to filter. A 0.0.0.0 field is ignored.	IP address
IP Mask	Type the IP mask to apply to the **Source: IP Addr** field.	IP mask
Port #	Type the source port of the packets you want to filter. The range of this field is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the source port in the packet against the value given in **Source: Port #** field. Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**.	**None**
TCP Estab	This applies only when the IP Protocol field is 6, TCP. If **Yes**, the rule matches packets that want to establish TCP connection(s) (SYN=1 and ACK=0); else it is ignored.	**No** (default)
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be N/A.	**No** (default)

Table 7-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** – Only packets that match the rule parameters will be logged. **Action Not Matched** – Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	**None**
Action Matched	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

The following figure illustrates the logic flow of an IP filter.

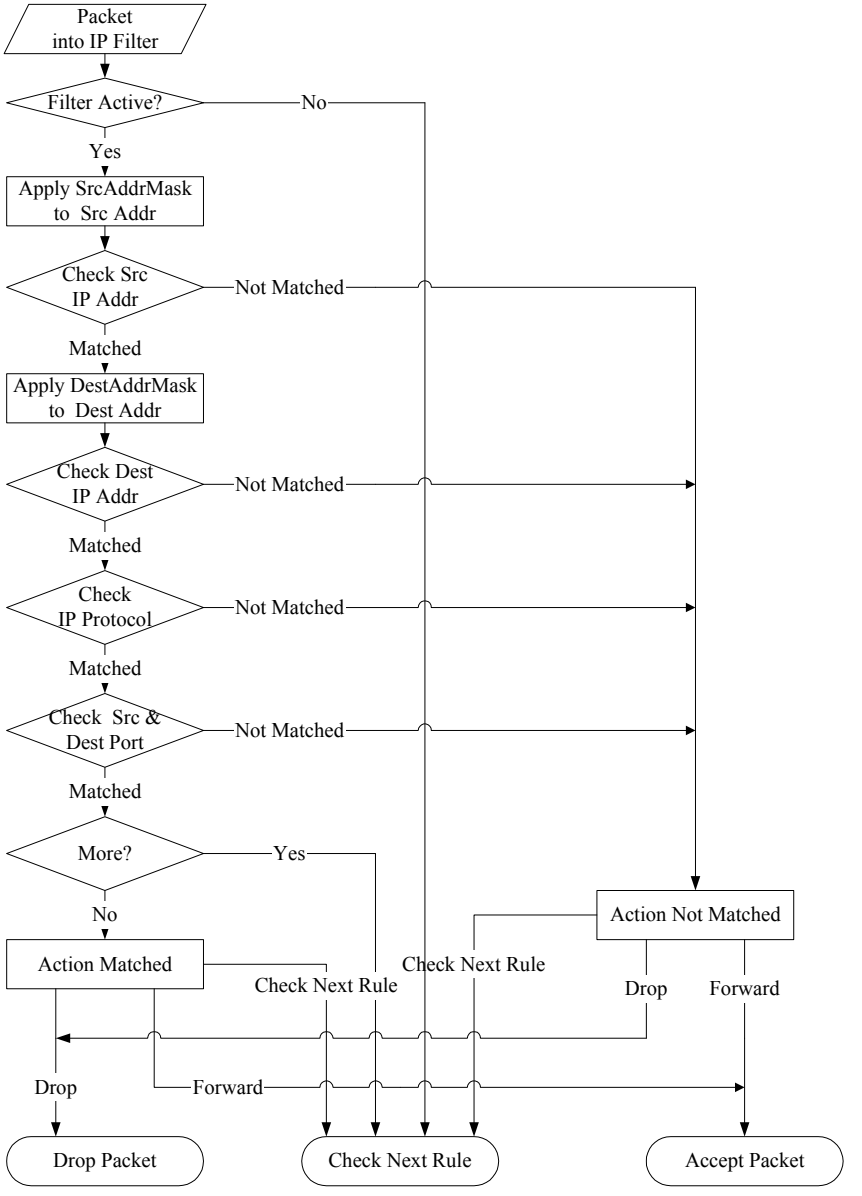

Figure 7-8 Executing an IP Filter

7.3.2 Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the ZyAIR treats a packet as a byte stream as opposed to an IP packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The ZyAIR applies the **Mask** (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** fields are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule select an empty filter set in menu 21, for example 4. Select **Generic Filter Rule** in the **Filter Type** field and press [ENTER] to open **Menu 21.4.1 – Generic Filter Rule**, as shown in the following figure.

```
                Menu 21.4.1 - Generic Filter Rule

                  Filter #: 4,1
                  Filter Type= Generic Filter Rule
                  Active= No
                  Offset= 0
                  Length= 0
                  Mask= N/A
                  Value= N/A
                  More= No            Log= None
                  Action Matched= Check Next Rule
                  Action Not Matched= Check Next Rule


              Press ENTER to Confirm or ESC to Cancel:
```

Figure 7-9 Menu 21.4.1 – Generic Filter Rule

The next table describes the fields in the Generic Filter Rule menu.

Table 7-4 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third rule of that set.	5,1
Filter Type	Press [SPACE BAR] and then [ENTER] to select a type of rule. Parameters displayed below each type will be different. Choices are **Generic Filter Rule** or **TCP/IP Filter Rule**.	**Generic Filter Rule**
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to turn on the filter rule.	**No** (default)

Table 7-4 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Offset	Type the starting byte of the data portion in the packet that you want to compare. The range for this field is from 0 to 255.	0 (default)
Length	Type the byte count of the data portion in the packet that you want to compare. The range for this field is 0 to 8.	0 (default)
Mask	Type the mask (in Hexadecimal) to apply to the data portion before comparison.	
Value	Type the value (in Hexadecimal) to compare with the data portion.	
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**.	**No** (default)
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** – Only matching packets and rules will be logged. **Action Not Matched** – Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	**None**
Action Matched	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**.	Check Next Rule
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**.	Check Next Rule
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

7.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** Device rules and Protocol Filter (**TCP/IP**) rules. Generic Filter rules act on the raw data from/to LAN and WAN. Protocol Filter rules act on IP packets.

When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the ZyAIR applies the protocol filters to the “native” IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic (or device)

filters are applied to the raw packets that appear on the wire. They are applied at the point where the ZyAIR is receiving and sending the packets; for instance, the interface. The interface can be an Ethernet, or any other hardware port. The following figure illustrates this.

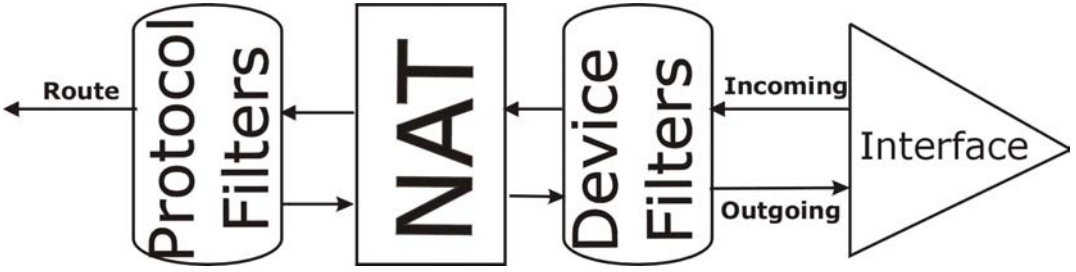

Figure 7-10 Protocol and Device Filter Sets

7.5 Example Filter

Let's look at an example to block outside users from telnetting into the ZyAIR.

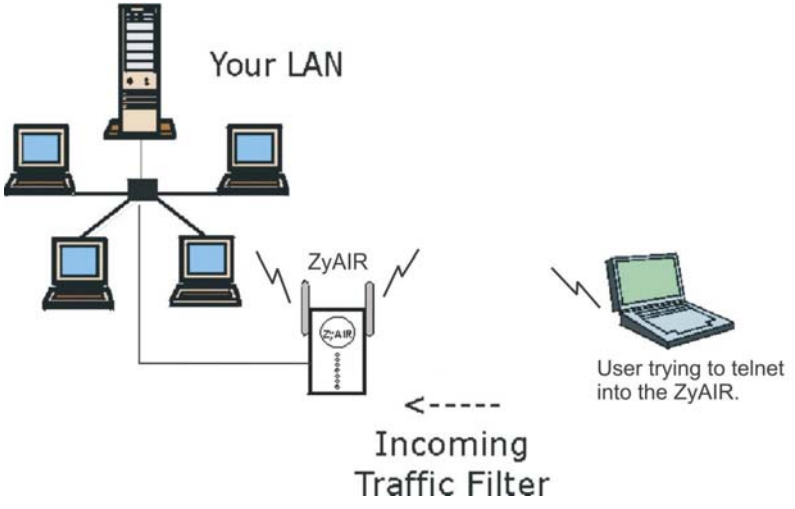

Figure 7-11 Sample Telnet Filter

Step 1. Enter 21 from the main menu to open **Menu 21 – Filter Set Configuration**.

Step 2. Enter the index number of the filter set you want to configure (in this example, 3).

Step 3. Type a descriptive name or comment in the **Edit Comments** field (for example, TELNET_WAN) and press [ENTER].

Step 4. Press [ENTER] at the message "Press ENTER to confirm or ESC to cancel" to open **Menu 21.3.1 – TCP/IP Filter Rule**.

Step 5. Type 1 to configure the first filter rule. Make the entries in this menu as shown next.

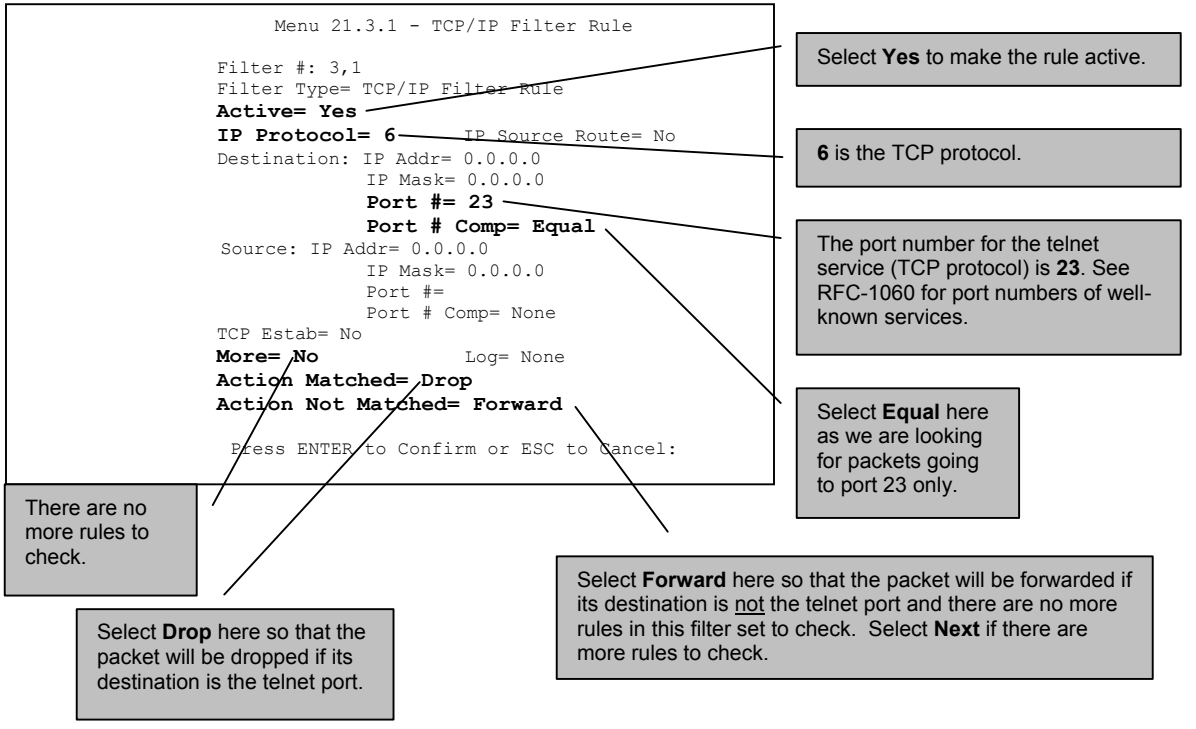
Menu 21.3.1 - TCP/IP Filter Rule
Filter #: 3,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6 IP Source Route= No
Destination: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #= 23
Port # Comp= Equal
Source: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #=
Port # Comp= None
TCP Estab= No
More= No Log= None
Action Matched= Drop
Action Not Matched= Forward
Press ENTER to Confirm or ESC to Cancel:
Select Yes to make the rule active.
6 is the TCP protocol.
The port number for the telnet service (TCP protocol) is 23. See RFC-1060 for port numbers of well-known services.
Select Equal here as we are looking for packets going to port 23 only.
There are no more rules to check.
Select Drop here so that the packet will be dropped if its destination is the telnet port.
Select Forward here so that the packet will be forwarded if its destination is not the telnet port and there are no more rules in this filter set to check. Select Next if there are more rules to check.

Figure 7-12 Sample Filter – Menu 21.3.1

When you press [ENTER] to confirm, the following screen appears. Note that there is only one filter rule in this set.

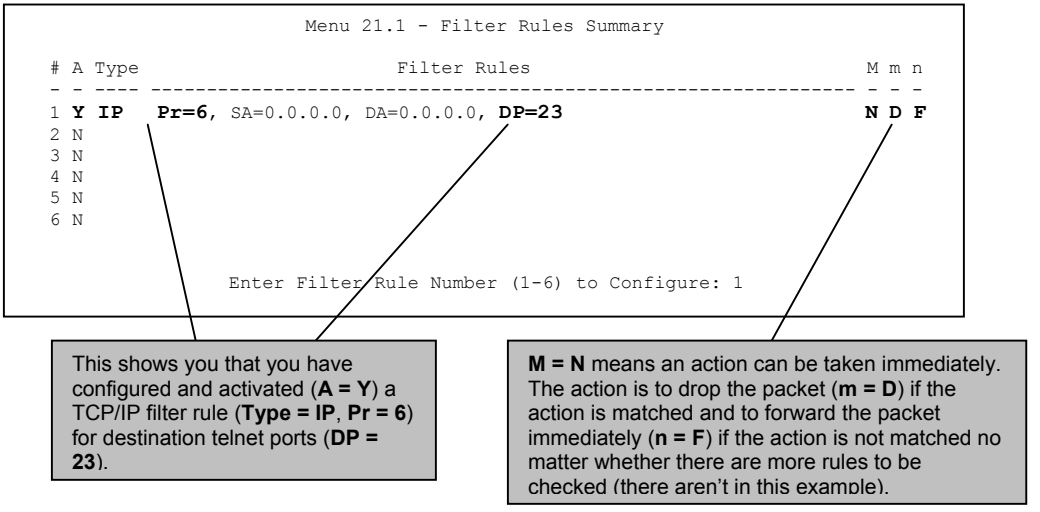
Menu 21.1 - Filter Rules Summary
A Type Filter Rules M m n
1 Y IP Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23 N D F
2 N
3 N
4 N
5 N
6 N
Enter Filter Rule Number (1-6) to Configure: 1
This shows you that you have configured and activated (A = Y) a TCP/IP filter rule (Type = IP, Pr = 6) for destination telnet ports (DP = 23).
M = N means an action can be taken immediately. The action is to drop the packet (m = D) if the action is matched and to forward the packet immediately (n = F) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

Figure 7-13 Sample Filter Rules Summary - Menu 21.1

After you have created the filter set, you must apply it.

Step 1. Enter 11 in the main menu to display menu 11 and type the remote node number to edit.

Step 2. Go to the **Edit Filter Sets** field, press [SPACE BAR] to choose **Yes** and press [ENTER].

Step 3. This brings you to menu 11.5. Apply the example filter set (for example, filter set 3) in this menu as shown in the next section.

7.6 Applying Filters and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them). Sets of factory default filter rules have been configured in menu 21 (but have not been applied) to filter traffic.

Table 7-5 Filter Sets Table

FILTER SETS	DESCRIPTION
Input Filter Sets:	Apply filters for incoming traffic. You may apply protocol or device filter rules. See earlier in this chapter for information on filters.
Output Filter Sets:	Apply filters for traffic leaving the ZyAIR. You may apply filter rules for protocol or device filters. See earlier in this section for information on types of filters.
Call Filter Sets:	Apply filters to decide if a packet should be allowed to trigger a call.

7.6.1 Ethernet Traffic

You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and type the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by typing their numbers separated by commas, for example, 3, 4, 6, 11. The factory default filter set, NetBIOS_LAN, is inserted in the **protocol filters** field under **Input Filter Sets** in menu 3.1 in order to prevent local NetBIOS messages from triggering calls to the DNS server.

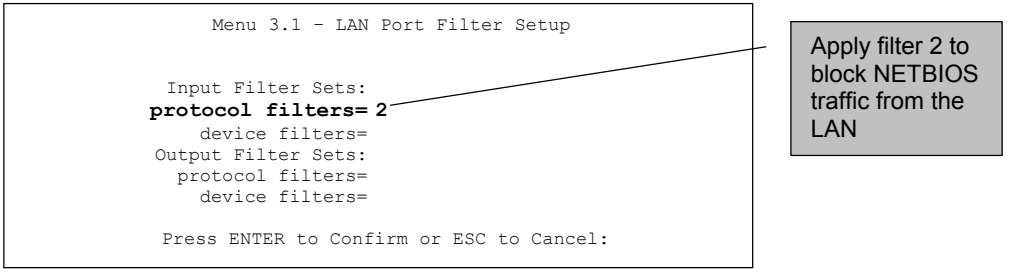
Menu 3.1 - LAN Port Filter Setup
Input Filter Sets:
protocol filters= 2
device filters=
Output Filter Sets:
protocol filters=
device filters=
Press ENTER to Confirm or ESC to Cancel:
Apply filter 2 to block NETBIOS traffic from the LAN

Figure 7-14 Filtering Ethernet Traffic

7.6.2 Remote Node Filters

Go to menu 11.5 (shown next) and type the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by typing their numbers separated by commas. The factory default filter set, NetBIOS_WAN, is inserted in the **protocol filters** field under **Call Filter Sets** in menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP.

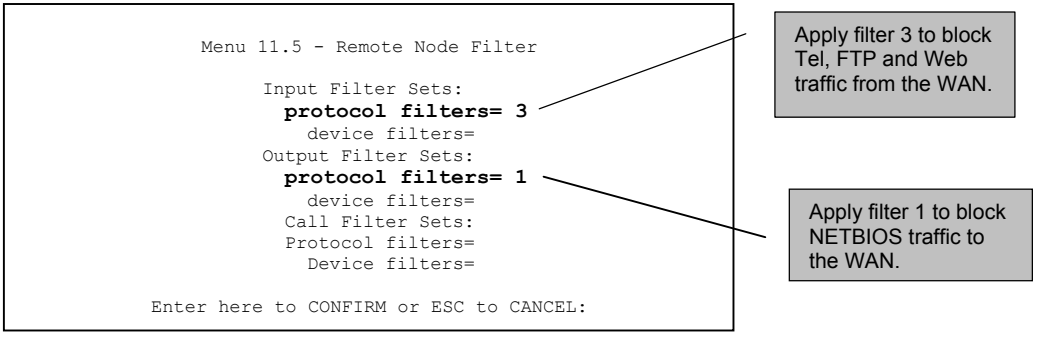
Menu 11.5 - Remote Node Filter
Input Filter Sets:
protocol filters= 3
device filters=
Output Filter Sets:
protocol filters= 1
device filters=
Call Filter Sets:
Protocol filters=
Device filters=
Enter here to CONFIRM or ESC to CANCEL:
Apply filter 3 to block Tel, FTP and Web traffic from the WAN.
Apply filter 1 to block NETBIOS traffic to the WAN.

Figure 7-15 Filtering Remote Node Traffic

Note that call filter sets are visible when you select PPTP or PPPoE encapsulation.

Chapter 8
SNMP Configuration

This chapter explains SNMP Configuration menu 22.

SNMP is only available if TCP/IP is configured.

8.1 About SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyAIR supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyAIR through the network. The ZyAIR supports SNMP version one (SNMPv1). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

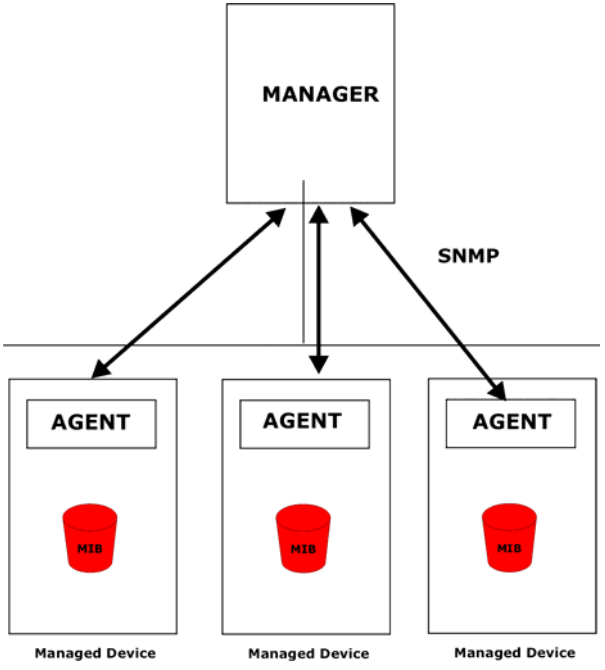

Figure 8-1 SNMP Management Model

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyAIR). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

8.2 Supported MIBs

The ZyAIR supports RFC-1215 and MIB II as defined in RFC-1213. The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

8.3 SNMP Configuration

To configure SNMP, select option 22 from the main menu to open **Menu 22 – SNMP Configuration** as shown next. The “community” for Get, Set and Trap fields is SNMP terminology for password.

```
                    Menu 22 - SNMP Configuration

                SNMP:
                  Get Community= public
                  Set Community= public
                  Trusted Host= 0.0.0.0
                  Trap:
                    Community= public
                    Destination= 0.0.0.0


                  Press ENTER to Confirm or ESC to Cancel:
```

Figure 8-2 Menu 22 – SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 8-1 SNMP Configuration Menu Fields

FIELD	DESCRIPTION	EXAMPLE
SNMP:		
Get Community	Type the **Get Community**, which is the password for the incoming Get- and GetNext requests from the management station.	public
Set Community	Type the **Set** community, which is the password for incoming Set requests from the management station.	public
Trusted Host	If you enter a trusted host, your ZyAIR will only respond to SNMP messages from this address. A blank (default) field means your ZyAIR will respond to all SNMP messages it receives, regardless of source.	0.0.0.0
Trap:		public
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.	
Destination	Type the IP address of the station to send your SNMP traps to.	0.0.0.0
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

8.4 SNMP Traps

The ZyAIR will send traps to the SNMP manager when any one of the following events occurs:

Table 8-2 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (*defined in RFC-1215*)	A trap is sent after booting (power on).
2	warmStart (*defined in RFC-1215*)	A trap is sent after booting (software reboot).
3	linkUp (*defined in RFC-1215*)	A trap is sent with the port number.
4	authenticationFailure (*defined in RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with wrong community (password).
6	linkDown (*defined in RFC-1215*)	A trap is sent with the port number when any of the links are down. See the following table.

The port number is its interface index under the interface group.

Table 8-3 Ports and Permanent Virtual Circuits

PORT	PVC (PERMANENT VIRTUAL CIRCUIT)
1	Ethernet LAN
2	1
3	2
…	…
13	12
14	xDSL

Chapter 9
System Information and Diagnosis

This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.4.

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type 24 in the main menu to open **Menu 24** - **System Maintenance**, as shown in the following figure.

```
                Menu 24 - System Maintenance

          1.  System Status
          2.  System Information and Console Port Speed
          3.  Log and Trace
          4.  Diagnostic
          5.  Backup Configuration
          6.  Restore Configuration
          7.  Upload Firmware
          8.  Command Interpreter Mode
          9.  Call Control
          10. Time and Date Setting
          11. Remote Management Setup


            Enter Menu Selection Number:
```

Figure 9-1 Menu 24 - System Maintenance

9.1 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown in the next figure. System Status is a tool that can be used to monitor your ZyAIR. Specifically, it gives you information on your LAN and Wireless LAN status, number of packets sent and received.

To get to System Status, type 24 to go to **Menu 24** – **System Maintenance.** From this menu, type 1**. System Status**. There are two commands in **Menu 24.1** – **System Maintenance** – **Status**. Entering 1 resets the counters; pressing [ESC] takes you back to the previous screen.

```
        Menu 24.1 - System Maintenance - Status           04:27:14
                                                          Sat. Jan. 01, 2000

 Port   Status        TxPkts      RxPkts    Cols    Tx B/s    Rx B/s     Up Time
  WAN   100M/Full       2138           0       0         0         0     4:27:12
  LAN   100M/Full       1205        1762       0         0         0     4:27:12
 WLAN    11M             656         354       0         0         0     4:27:12

 Port   Ethernet Address        IP Address           IP Mask       DHCP
  WAN  00:A0:C5:00:15:38          0.0.0.0           0.0.0.0     Client
  LAN  00:A0:C5:00:15:37      192.168.1.1     255.255.255.0     Server
 WLAN  00:A0:C5:00:15:37

      System up Time:     4:27:18

                                  Press Command:

               COMMANDS: 1-Drop WAN 9-Reset Counters   ESC-Exit
```

Figure 9-2 Menu 24.1 – System Maintenance – Status

The following table describes the fields present in **Menu 24.1** – **System Maintenance** – **Status** which are read-only and meant for diagnostic purposes.

Table 9-1 System Maintenance – Status Menu Fields

FIELD	DESCRIPTION
Port	This is the port type. Port types are: LAN, WAN and WLAN
Status	Shows the status of the port.
TxPkts	The number of transmitted packets to this remote node.
RxPkts	The number of received packets from this remote node.
Cols	The number of collisions on this connection.
Tx B/s	Shows the transmission rate in bytes per second.
Rx B/s	Shows the receiving rate in bytes per second.
Up Time	Time this channel has been connected to the current remote node.
Ethernet Address	Shows the MAC address of the port.
IP Address	Shows the IP address of the network device connected to the port.
IP Mask	Shows the subnet mask of the network device connected to the port.
DHCP	Shows the DHCP setting (None, Relay or Server) of the network device connected to the port.
System Up Time	The time the ZyAIR is up and running from the last reboot.

9.2 System Information

To get to the System Information:

Step 1. Enter 24 to display **Menu 24** – **System Maintenance**.

Step 2. Enter 2 to display **Menu 24.2** – **System Information and Console Port Speed**.

Step 3. From this menu you have two choices as shown in the next figure:

```
Menu 24.2 - System Information and Console Port Speed
        1. System Information
        2. Console Port Speed


                Please enter selection:
```

Figure 9-3 Menu 24.2 – System Information and Console Port Speed

9.2.1 System Information

Enter 1 in menu 24.2 to display the screen shown next.

```
Menu 24.2.1 - System Maintenance - Information

   Name:
   Routing: IP
   ZyNOS F/W Version: V3.50(HB.0)b2 | 07/25/2002


   LAN
     Ethernet Address: 00:A0:C5:00:15:37
     IP Address: 192.168.1.1
     IP Mask: 255.255.255.0
     DHCP: Server

         Press ESC or RETURN to Exit:
```

Figure 9-4 Menu 24.2.1 – System Maintenance – Information

Table 9-2 Fields in System Maintenance

FIELD	DESCRIPTION
Name	Displays the system name of your ZyAIR. This information can be changed in **Menu 1 – General Setup**.
Routing	Refers to the routing protocol used.

Table 9-2 Fields in System Maintenance

FIELD	DESCRIPTION
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your ZyAIR.
IP Address	This is the IP address of the ZyAIRe in dotted decimal notation.
IP Mask	This shows the subnet mask of the ZyAIR.
DHCP	This field shows the DHCP setting of the ZyAIR.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

9.2.2 Console Port Speed

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your ZyAIR supports 9600 (default), 19200, 38400 and 57600bps console port speeds. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

```
Menu 24.2.2 - System Maintenance - Change Console Port Speed

                    Console Port Speed: 9600

                Press ENTER to Confirm or ESC to Cancel:
```

Figure 9-5 Menu 24.2.2 – System Maintenance – Change Console Port Speed

After you changed the console port speed on your ZyAIR, you must also make the same change to the console port speed parameter of your communication software.

9.3 Log and Trace

There are two logging facilities in the ZyAIR. The first is the error logs and trace records that are stored locally. The second is the UNIX syslog facility for message logging.

9.3.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error log. Follow the procedures to view the local error/trace log:

Step 1. Type 24 in the main menu to display **Menu 24** – **System Maintenance**.

Step 2. From menu 24, type 3 to display **Menu 24.3** – **System Maintenance** – **Log and Trace**.

```
Menu 24.3 - System Maintenance - Log and Trace

                1. View Error Log
                2. UNIX Syslog and Accounting

                4. Call-Triggering Packet
```

Figure 9-6 Menu 24.3 – System Maintenance – Log and Trace

Step 3. Enter 1 from **Menu 24.3** – **System Maintenance** – **Log and Trace** and press [ENTER] twice to display the error log in the system.

After the ZyAIR finishes displaying the error log, you will have the option to clear it. Samples of typical error and information messages are presented in the next figure.

```
 45 Sat Jan  1 00:00:00 2000 PP0e  INFO  LAN promiscuous mode <1>
 46 Sat Jan  1 00:00:00 2000 PINI  INFO  Last errorlog repeat 1 Times
 47 Sat Jan  1 00:00:00 2000 PINI  INFO  main: init completed
 48 Sat Jan  1 00:00:02 2000 PP05 -WARN  SNMP TRAP 3: link up
 49 Sat Jan  1 00:00:02 2000 PP16 -WARN  Last errorlog repeat 2 Times
 50 Sat Jan  1 00:00:02 2000 PP16  INFO  adjtime task pause 1 day
 51 Sat Jan  1 00:00:30 2000 PSSV -WARN  SNMP TRAP 0: cold start
 52 Sat Jan  1 00:32:34 2000 PP10  INFO  SMT Password pass
 53 Sat Jan  1 00:32:34 2000 PINI  INFO  SMT Session Begin
 54 Sat Jan  1 00:32:55 2000 PINI  INFO  SMT Session End

Clear Error Log (y/n):
```

Figure 9-7 Sample Error and Information Messages

9.3.2 UNIX Syslog

The ZyAIR uses the UNIX syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog can be configured in **Menu 24.3.2** – **System Maintenance** – **UNIX Syslog**, as shown next.

```
                Menu 24.3.2 - System Maintenance - UNIX Syslog

                   Syslog:
                   Active= No
                   Syslog IP Address= ?
                   Log Facility= Local 1

                   Types:
                   CDR= No
                   Packet triggered= No
                   Filter log= No
                   PPP log= No

              Press ENTER to Confirm or ESC to Cancel:
```

Figure 9-8 Menu 24.3.2 – System Maintenance – Syslog

You need to configure the UNIX syslog parameters described in the following table to activate syslog and then choose what you want to log.

Table 9-3 System Maintenance Menu – Syslog Parameters

PARAMETER	DESCRIPTION
UNIX Syslog:	
Active	Press [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog IP address	Type the IP address of your syslog server.
Log Facility	Press [SPACE BAR] and then [ENTER] to select one of seven different local options. The log facility lets you log the message in different server files. Refer to your UNIX manual.
Types:	
CDR	Call Detail Record (CDR) logs all data phone line activity if set to **Yes**.
Packet Triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to **Yes**.
Filter Log	No filters are logged when this field is set to **No**. Filters with the individual filter Log Filter field set to **Yes** are logged when this field is set to **Yes**.
PPP Log	PPP events are logged when this field is set to **Yes**.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

9.3.3 Call-Triggering Packet

Call-Triggering Packet displays information about the packet that triggered a dial-out call in an easy readable format. Equivalent information is available in menu 24.1 in hex format.

9.4 Diagnostic

The diagnostic facility allows you to test the different aspects of your ZyAIR to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in the following figure.

```
                Menu 24.4 - System Maintenance - Diagnostic

                TCP/IP
                  1. Ping Host
                  2. WAN DHCP Release
                  3. WAN DHCP Renewal
                  4. Internet Setup Test

                System
                  11. Reboot System

                  Enter Menu Selection Number:
                  Host IP Address= N/A
```

Figure 9-9 Menu 24.4 – System Maintenance – Diagnostic

Follow the procedure next to get to display this menu:

Step 1. From the main menu, type 24 to open **Menu 24 – System Maintenance**.

Step 2. From this menu, type 4. Diagnostic to open **Menu 24.4** – **System Maintenance** – **Diagnostic**.

The table below describes the diagnostic tests available in menu 24.4 for your ZyAIR and the connections.

Table 9-4 System Maintenance Menu – Diagnostic

FIELD	DESCRIPTION
Ping Host	Ping the host to see if the links and TCP/IP protocol on both systems are working.
DHCP Release	Release the IP address assigned by the DHCP server.
DHCP Renewal	Get a new IP address from the DHCP server.
Internet Setup Test	Use this option to test your Internet connection.
Reboot System	Reboot the ZyAIR.
Host IP Address	If you typed 1 to ping host, now type the address of the computer you want to ping.

Chapter 10
Firmware and Configuration File Maintenance

This chapter tells you how to back up and restore your configuration file as well as upload new firmware and a new configuration file.

10.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the ZyAIR's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```
This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the ZyAIR.

```
ftp> get rom-0 config.cfg
```
This is a sample FTP session saving the current configuration to the computer file "config.cfg".

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyAIR only recognizes "rom-0" and "ras". Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyAIR and the external filename refers to the filename not on the ZyAIR, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **ZyNOS F/W Version** field in **Menu 24.2.1 – System Maintenance – Information** to confirm that you have uploaded the correct firmware version. The AT command is the command you enter after you press "y" when prompted in the SMT menu to go into debug mode.

Table 10-1 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the ZyAIR. Uploading the rom-0 file replaces the entire ROM file system, including your ZyAIR configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the ZyAIR.	*.bin

10.2 Backup Configuration

The ZyAIR displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2; depending on whether you use the console port or Telnet.

Option 5 from **Menu 24 – System Maintenance** allows you to backup the current ZyAIR configuration to your computer. Backup is highly recommended once your ZyAIR is functioning properly. FTP is the preferred methods for backing up your current configuration to your computer since they are faster. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files.

Please note that terms "download" and "upload" are relative to the computer. Download means to transfer from the ZyAIR to the computer, while upload means from your computer to the ZyAIR.

10.2.1 Backup Configuration

Follow the instructions as shown in the next screen.

```
                Menu 24.5 - System Maintenance - Backup Configuration

To transfer the configuration file to your workstation, follow the procedure
below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and
   SMT password as requested.
3. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current router configuration to
   your workstation.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your router manual.


                                Press ENTER to Exit:
```

Figure 10-1 Telnet in Menu 24.5

10.2.2 Using the FTP Command from the Command Line

Step 1. Launch the FTP client on your computer.

Step 2. Enter “open”, followed by a space and the IP address of your ZyAIR.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is “1234”).

Step 5. Enter “bin” to set transfer mode to binary.

Step 6. Use “get” to transfer files from the ZyAIR to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the ZyAIR to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.

Step 7. Enter “quit” to exit the ftp prompt.

10.2.3 Example of FTP Commands from the Command Line

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 10-2 FTP Session Example

10.2.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 10-2 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

10.2.5 TFTP and FTP over WAN Will Not Work When

TFTP, FTP and Telnet over WAN will not work when:

1. You have disable Telnet service in menu 24.11.
2. You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.

3. The IP address in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the ZyAIR will disconnect the Telnet session immediately.
4. You have an SMT console session running.

10.2.6 Backup Configuration Using TFTP

The ZyAIR supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

Step 1. Use telnet from your computer to connect to the ZyAIR and log in. Because TFTP does not have any security checks, the ZyAIR records the IP address of the telnet client and accepts TFTP requests only from this address.

Step 2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24** – **System Maintenance**.

Step 3. Enter command "sys stdio 0" to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command "sys stdio 5" to restore the five-minute SMT timeout (default) when the file transfer is complete.

Step 4. Launch the TFTP client on your computer and connect to the ZyAIR. Set the transfer mode to binary before starting data transfer.

Step 5. Use the TFTP client (see the example below) to transfer files between the ZyAIR and the computer. The file name for the configuration file is "rom-0" (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "get" to transfer from the ZyAIR to the computer and "binary" to set binary transfer mode.

10.2.7 TFTP Command Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the ZyAIR IP address, "get" transfers the file source on the ZyAIR (rom-0, name of the configuration file on the ZyAIR) to the file destination on the computer and renames it config.rom.

10.2.8 GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 10-3 General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyAIR. 192.168.1.1 is the ZyAIR's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the ZyAIR and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyAIR. The filename for the firmware is "ras" and for the configuration file, is "rom-0".
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

Refer to *section 10.2.5* to read about configurations that disallow TFTP and FTP over WAN.

10.2.9 Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

Step 1. Display menu 24.5 and enter "y" at the following screen.

```
Ready to backup Configuration via Xmodem.
Do you want to continue (y/n):
```

Figure 10-3 System Maintenance – Backup Configuration

Step 2. The following screen indicates that the Xmodem download has started.

```
You can enter ctrl-x to terminate operation any time.
Starting XMODEM download...
```

Figure 10-4 System Maintenance – Starting Xmodem Download Screen

Step 3. Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

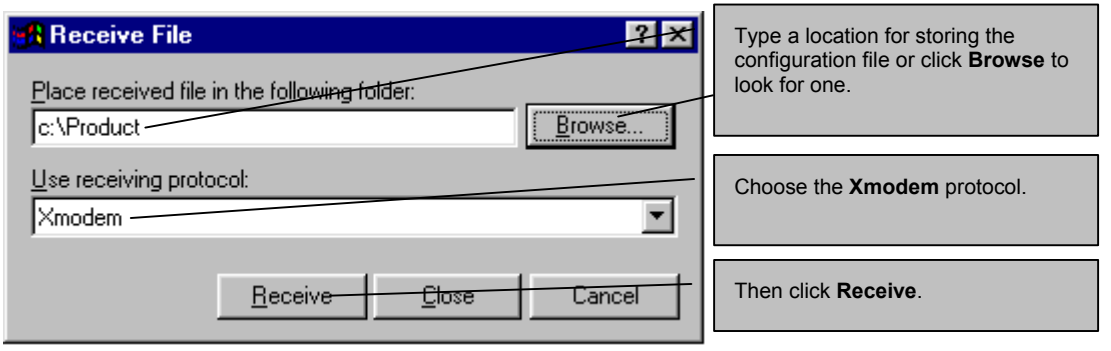

Figure 10-5 Backup Configuration Example

Step 4. After a successful backup you will see the following screen. Press any key to return to the SMT menu.

```
** Backup Configuration completed. OK.
### Hit any key to continue.###
```

Figure 10-6 Successful Backup Confirmation Screen

10.3 Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your ZyAIR since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

WARNING!
DO NOT INTERUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR ZYAIR. WHEN THE RESTORE CONFIGURATION PROCESS IS COMPLETE, THE ZYAIR WILL AUTOMATICALLY RESTART.

10.3.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

```
                Menu 24.6 -- System Maintenance - Restore Configuration

To transfer the firmware and configuration file to your workstation, follow the procedure
below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and
   SMT password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of
   your backup configuration file on your workstation and rom-0 is the
   remote file name on the router. This restores the configuration to
   your router.
4. The system reboots automatically after a successful file transfer

For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your router manual.


                                    Press ENTER to Exit:
```

Figure 10-7 Telnet into Menu 24.6

Step 1. Launch the FTP client on your computer.

Step 2. Enter “open”, followed by a space and the IP address of your ZyAIR.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is “1234”).

Step 5. Enter “bin” to set transfer mode to binary.

Step 6. Find the “rom” file (on your computer) that you want to restore to your ZyAIR.

Step 7. Use “put” to transfer files from the ZyAIR to the computer, for example, “put config.rom rom-0” transfers the configuration file “config.rom” on your computer to the ZyAIR. See earlier in this chapter for more information on filename conventions.

Step 8. Enter “quit” to exit the ftp prompt. The ZyAIR will automatically restart after a successful restore process.

10.3.2 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Figure 10-8 Restore Using FTP Session Example

Refer to *section 10.2.5* to read about configurations that disallow TFTP and FTP over WAN.

10.3.3 Restore Via Console Port

Restore configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

Step 1. Display menu 24.6 and enter "y" at the following screen.

```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

Figure 10-9 System Maintenance – Restore Configuration

Step 2. The following screen indicates that the Xmodem download has started.

```
Starting XMODEM download (CRC mode) ...
CCCCCCCCC
```

Figure 10-10 System Maintenance – Starting Xmodem Download Screen

Step 3. Run the HyperTerminal program by clicking **Transfer**, then **Send File** as shown in the following screen.

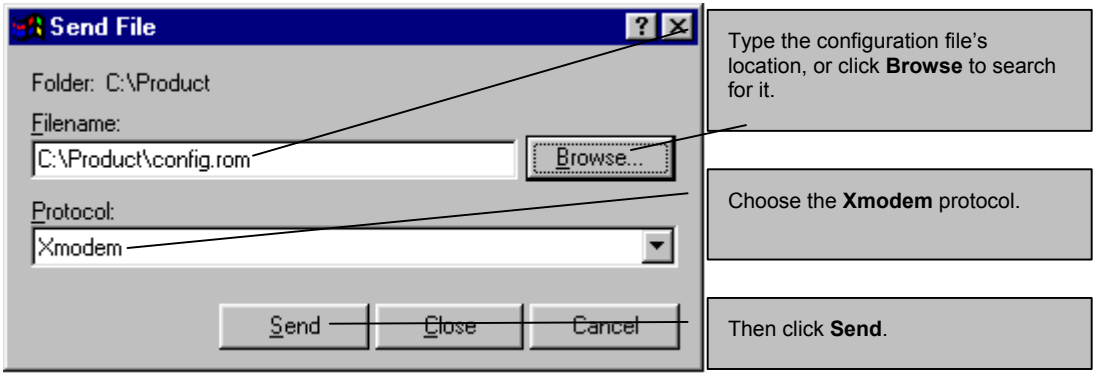

Figure 10-11 Restore Configuration Example

Step 4. After a successful restoration you will see the following screen. Press any key to restart the ZyAIR and return to the SMT menu.

```
Save to ROM
Hit any key to start system reboot.
```

Figure 10-12 Successful Restoration Confirmation Screen

10.4 Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the previous *Restore Configuration* section or by following the instructions in **Menu 24.7.2 – System Maintenance – Upload System Configuration File** (for console port).

WARNING!
DO NOT INTERUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR ZYAIR.

10.4.1 Firmware File Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the ZyAIR, you will see the following screens for uploading firmware and the configuration file using FTP.

```
                Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
  3. Type "put firmwarefilename ras" where "firmwarefilename" is the name
     of your firmware upgrade file on your workstation and "ras" is the
     remote file name on the system.
  4. The system reboots automatically after a successful firmware upload.


For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.


                                    Press ENTER to Exit:
```

Figure 10-13 Telnet Into Menu 24.7.1 – Upload System Firmware

10.4.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

```
            Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
  3. Type "put configurationfilename rom-0" where "configurationfilename"
     is the name of your system configuration file on your workstation, which
     will be transferred to the "rom-0" file on the system.
  4. The system reboots automatically after the upload system configuration
     file process is complete.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.

                                    Press ENTER to Exit:
```

Figure 10-14 Telnet Into Menu 24.7.2 – System Maintenance

To upload the firmware and the configuration file, follow these examples

10.4.3 FTP File Upload Command from the DOS Prompt Example

Step 1. Launch the FTP client on your computer.

Step 2. Enter "open", followed by a space and the IP address of your ZyAIR.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is "1234").

Step 5. Enter "bin" to set transfer mode to binary.

Step 6. Use "put" to transfer files from the computer to the ZyAIR, for example, "put firmware.bin ras" transfers the firmware on your computer (firmware.bin) to the ZyAIR and renames it "ras". Similarly, "put config.rom rom-0" transfers the configuration file on your computer (config.rom) to the ZyAIR and renames it "rom-0". Likewise "get rom-0 config.rom" transfers the configuration file on the ZyAIR to your computer and renames it "config.rom." See earlier in this chapter for more information on filename conventions.

Step 7. Enter "quit" to exit the ftp prompt.

10.4.4 FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 10-15 FTP Session Example of Firmware File Upload

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to *section 10.2.5* to read about configurations that disallow TFTP and FTP over WAN.

10.4.5 TFTP File Upload

The ZyAIR also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

Step 1. Use telnet from your computer to connect to the ZyAIR and log in. Because TFTP does not have any security checks, the ZyAIR records the IP address of the telnet client and accepts TFTP requests only from this address.

Step 2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

Step 3. Enter the command "sys stdio 0" to disable the console timeout, so the TFTP transfer will not be interrupted. Enter "command sys stdio 5" to restore the five-minute console timeout (default) when the file transfer is complete.

Step 4. Launch the TFTP client on your computer and connect to the ZyAIR. Set the transfer mode to binary before starting data transfer.

Step 5. Use the TFTP client (see the example below) to transfer files between the ZyAIR and the computer. The file name for the firmware is "ras".

Note that the telnet connection must be active and the ZyAIR in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "get" to transfer from the ZyAIR to the computer, "put" the other way around, and "binary" to set binary transfer mode.

10.4.6 TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the ZyAIR's IP address and "put" transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the ZyAIR).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

10.4.7 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your ZyAIR. However, in the event of your network being down, uploading files is only possible with a direct connection to your ZyAIR via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

10.4.8 Uploading Firmware File Via Console Port

Step 1. Select 1 from **Menu 24.7** – **System Maintenance** – **Upload Firmware** to display **Menu 24.7.1 – System Maintenance – Upload System Firmware**, then follow the instructions as shown in the following screen.

```
            Menu 24.7.1 - System Maintenance - Upload System Firmware


        To upload system firmware:
        1. Enter "y" at the prompt below to go into debug mode.
        2. Enter "atur" after "Enter Debug Mode" message.
        3. Wait for "Starting XMODEM upload" message before activating
           Xmodem upload on your terminal.
        4. After successful firmware upload, enter "atgo" to restart the
           router.

        Warning: Proceeding with the upload will erase the current system
        firmware.
                         Do You Wish To Proceed:(Y/N)
```

Figure 10-16 Menu 24.7.1 as seen using the Console Port

Step 2. After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

10.4.9 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

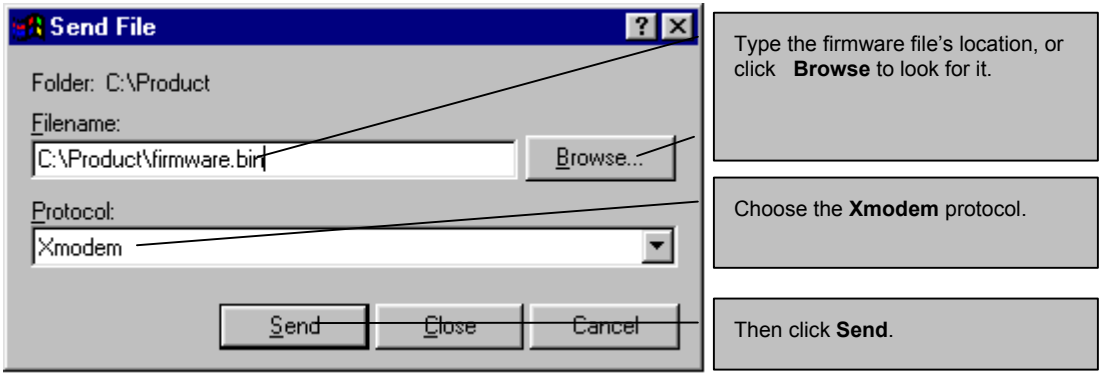

Figure 10-17 Example Xmodem Upload

After the firmware upload process has completed, the ZyAIR will automatically restart.

10.4.10 Uploading Configuration File Via Console Port

Step 1. Select 2 from **Menu 24.7** – **System Maintenance** – **Upload Firmware** to display **Menu 24.7.2 – System Maintenance – Upload System Configuration File**. Follow the instructions as shown in the next screen.

```
Menu 24.7.2 - System Maintenance - Upload System Configuration File


To upload system configuration file:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atlc" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart the
   system.

Warning:
1. Proceeding with the upload will erase the current
   configuration file.
2. The system's console port speed (Menu 24.2.2) may change
   when it is restarted; please adjust your terminal's speed
   accordingly. The password may change (menu 23), also.
3. When uploading the DEFAULT configuration file, the console
   port speed will be reset to 9600 bps and the password to
   "1234".
                Do You Wish To Proceed:(Y/N)
```

Figure 10-18 Menu 24.7.2 as seen using the Console Port

Step 2. After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

Step 3. Enter "atgo" to restart the ZyAIR.

10.4.11 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

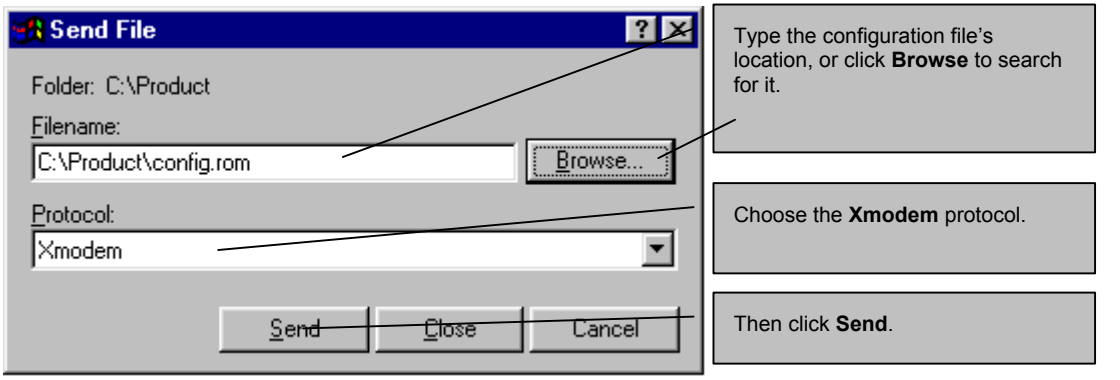

Figure 10-19 Example Xmodem Upload

After the configuration upload process has completed, restart the ZyAIR by entering "atgo".

Chapter 11
System Maintenance and Information

This chapter leads you through SMT menus 24.8 to 24.11.

11.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the zyxel.com web site for more detailed information on CI commands. Enter 8 from **Menu 24 – System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type `exit` to return to the SMT main menu when finished.

```
                Menu 24 - System Maintenance

              1.  System Status
              2.  System Information and Console Port Speed
              3.  Log and Trace
              4.  Diagnostic
              5.  Backup Configuration
              6.  Restore Configuration
              7.  Upload Firmware
              8.  Command Interpreter Mode
              9.  Call Control
              10. Time and Date Setting
              11. Remote Management Setup


               Enter Menu Selection Number:
```

Figure 11-1 Menu 24 – System Maintenance

```
Copyright (c) 1994 - 2002 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            device          ether
poe             pptp            config          wlan
radius          ip              ppp             bridge
hdap            8021x
ras>
```

Figure 11-2 Valid CI Commands

11.2 Time and Date Setting

The ZyAIR keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyAIR. Menu 24.10 allows you to update the time and date settings of your ZyAIR. The real time is then displayed in the ZyAIR error logs and firewall logs.

Step 1. Select menu 24 in the main menu to open **Menu 24 – System Maintenance**.

Step 2. Then enter 10 to go to **Menu 24.10 – System Maintenance – Time and Date Setting** to update the time and date settings of your ZyAIR as shown in the following screen.

```
        Menu 24.10 - System Maintenance - Time and Date Setting

Use Time Server when Bootup= NTP (RFC-1305)
Time Server Address= 128.105.39.21

Current Time:                          05 : 47 : 19
New Time (hh:mm:ss):                   05 : 47 : 17

Current Date:                          2000 - 01 - 01
New Date (yyyy-mm-dd):                 2000 - 01 - 01

Time Zone= GMT

Daylight Saving= No
Start Date (mm-dd):                          01 - 01
End Date (mm-dd):                            01 - 01


          Press ENTER to Confirm or ESC to Cancel:
```

Figure 11-3 Menu 24.10 System Maintenance – Time and Date Setting

Table 11-1 Time and Date Setting Fields

FIELD	DESCRIPTION
Use Time Server when Bootup	Enter the time service protocol that your time server sends when you turn on the ZyAIR. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to **Time (RFC-868)**. **None**. The default, enter the time manually.

Table 11-1 Time and Date Setting Fields

FIELD	DESCRIPTION
Time Server Address	Enter the IP address or domain name of your time server. Check with your ISP/network administrator if you are unsure of this information.
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you re-enter this menu.
New Date	Enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	If you use daylight savings time, then choose **Yes**.
Start Date	If using daylight savings time, enter the month and day that it starts on.
End Date	If using daylight savings time, enter the month and day that it ends on
Once you have filled in this menu, press [ENTER] at the message “Press ENTER to Confirm or ESC to Cancel“ to save your configuration, or press [ESC] to cancel.	

11.2.1 Resetting the Time

The ZyAIR resets the time in three instances:

i. On leaving menu 24.10 after making changes.

ii. When the ZyAIR starts up, if there is a time server configured in menu 24.10.

iii. 24-hour intervals after starting.

Chapter 12
Call Scheduling

Call scheduling (applicable for PPPoE or PPTP encapsulation only) allows you to dictate when a remote node should be called and for how long.

12.1 Introduction

The call scheduling feature allows the ZyAIR to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a video cassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 – Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 – Schedule Setup** as shown next.

```
                        Menu 26 - Schedule Setup

Schedule                                Schedule
Set #          Name                     Set #          Name
------  -----------------               ------  -----------------
  1      _________________                 7      _________________
  2      _________________                 8      _________________
  3      _________________                 9      _________________
  4      _________________                10      _________________
  5      _________________                11      _________________
  6      _________________                12      _________________


               Enter Schedule Set Number to Configure= 0

               Edit Name= N/A

               Press ENTER to Confirm or ESC to Cancel:
```

Figure 12-1 Menu 26 - Schedule Setup

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2 ,3 and 4 in are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the ZyAIR, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

To delete a schedule set, enter the set number and press [SPACE BAR] **and then** [ENTER] **(or delete) in the** Edit Name **field.**

To setup a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 - Schedule Set Setup** as shown next.

```
                    Menu 26.1 Schedule Set Setup

Active= Yes
Start Date(yyyy-mm-dd)= 2000 - 01 - 01
How Often= Once
Once:
  Date(yyyy-mm-dd)= 2000 - 01 - 01
Weekdays:
  Sunday= N/A
  Monday= N/A
  Tuesday= N/A
  Wednesday= N/A
  Thursday= N/A
  Friday= N/A
  Saturday= N/A
Start Time(hh:mm)= 00 : 00
Duration(hh:mm)= 00 : 00
Action= Forced On

          Press ENTER to Confirm or ESC to Cancel:
```

Figure 12-2 Schedule Set Setup

If a connection has been already established, your ZyAIR will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

Table 12-1 Schedule Set Setup Fields

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] to **No** and press [ENTER] to disable the schedule set.	**Yes**
Start Date	Enter the start date when you wish the set to take effect in year - month-date format. Valid dates are from the present to 2036-February-5.	2000-01-01
How Often	Should this schedule set recur weekly or be used just once only? Press [SPACE BAR] and then [ENTER] to select **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses.	**Once**

FIELD	DESCRIPTION	EXAMPLE
Once: Date	If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format.	2000-01-01
Weekday: Day	If you selected **Weekly** in the **How Often** field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select **Yes**, then press [ENTER].	**Yes** **No** **N/A**
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.	09:00
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.	08:00
Action	**Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line.	**Forced On**
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the **Main Menu** and then enter the target remote node index. Using [SPACE BAR], select **PPPoE** or **PPTP** in the **Encapsulation** field and then press [ENTER] to make the schedule sets field available as shown next.

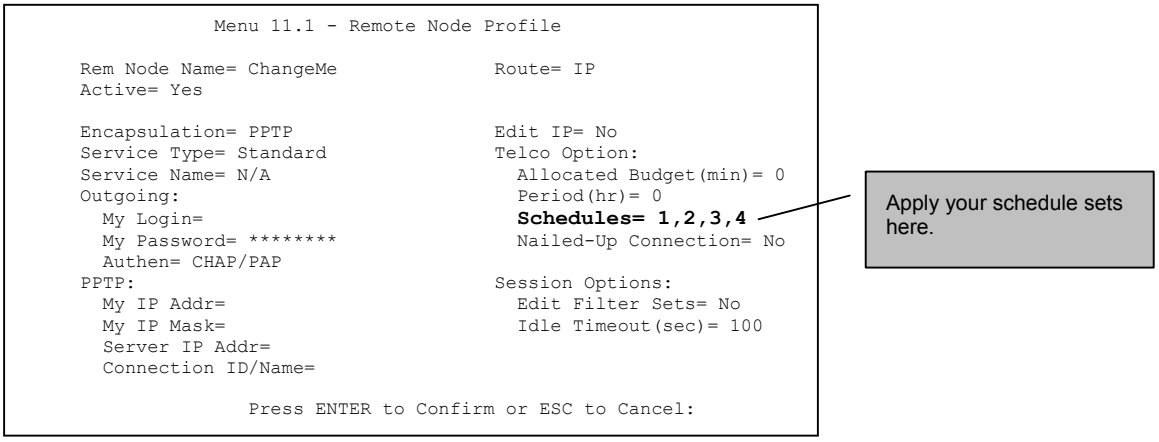

Figure 12-3 Applying Schedule Set(s) to a Remote Node (PPTP)

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

Chapter 13
Remote Management

This chapter covers remote management (SMT menu 24.11).

13.1 Telnet

You can configure your ZyAIR for remote Telnet access as shown next.

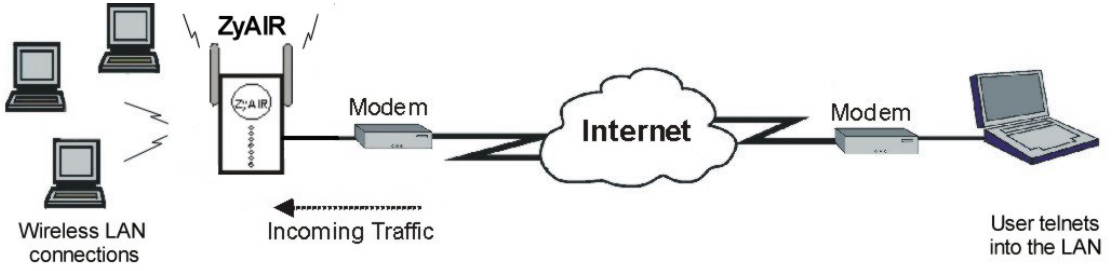

Figure 13-1 Telnet Configuration on a TCP/IP Network

13.2 FTP

You can upload and download ZyAIR firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

13.3 Web

You can use the ZyAIR's embedded web configurator for configuration and file management. See the *online help* for details.

13.4 Remote Management

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

Enter 11 from menu 24 to display **Menu 24.11 – Remote Management Control**.

13.4.1 Remote Management Setup

Remote management setup is for managing Telnet, FTP and Web services. You can customize the service port, access interface and the secured client IP address to enhance security and flexibility.

You may manage your ZyAIR from a remote location via:

the Internet (**WAN only**), the **LAN only**, **All** (LAN and WAN) or **Disable** (neither).

- WAN only (Internet)
- ALL (LAN and WAN)
- LAN only
- Disable (Neither)

If you enable remote management of a service, but have applied a filter to block the service, then you will not be able to remotely manage the service.

Enter 11, from menu 24, to display **Menu 24.11 - Remote Management Control** (shown next).

```
                Menu 24.11 - Remote Management Control

TELNET Server:     Port = 23         Access = LAN only
                   Secured Client IP = 0.0.0.0

FTP Server:        Port = 21         Access = LAN only
                   Secured Client IP = 0.0.0.0

Web Server:        Port = 80         Access = LAN only
                   Secured Client IP = 0.0.0.0

SNMP Service:      Port = 161        Access = ALL
                   Secured Client IP = 0.0.0.0

DNS Service:       Port = 53         Access = ALL
                   Secured Client IP = 0.0.0.0


              Press ENTER to Confirm or ESC to Cancel:
```

Figure 13-2 Menu 24.11 - Remote Management Control

Table 13-1 Menu 24.11 -Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
Telnet Server FTP Server Web Server SNMP Service DNS Service	Each of these read-only labels denotes a server or service that you may use to remotely manage the ZyAIR.	

Table 13-1 Menu 24.11 -Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
Port	This field shows the port number for the remote management service. You may change the port number for a service if needed, but you must use the same port number to use that service for remote management. The DNS Service port number is 53. This cannot be changed.	
Access	Select the access interface (if any) by pressing the [SPACE BAR]. Choices are: **LAN only**, **WAN only**, **All** or **Disable**. The default is **LAN only**.	LAN only
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the ZyAIR. Enter an IP address to restrict access to a client with a matching IP address.	0.0.0.0
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.		

13.4.2 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in menu 24.11.
3. The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the ZyAIR will disconnect the session immediately.
4. There is already another remote management session of the same type (Telnet, FTP or Web) running. You may only have one remote management session of the same type running at one time.
5. There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.

13.5 Remote Management and NAT

When NAT is enabled:

- Use the ZyAIR's WAN IP address when configuring from the WAN.
- Use the ZyAIR's LAN IP address when configuring from the LAN.

13.6 System Timeout

There is a system timeout of five minutes (300 seconds) for Telnet/web/FTP connections. Your ZyAIR will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

Part: IV

ADDITIONAL INFORMATION

This part contains Troubleshooting, Appendices and the Index.

Chapter 14
Troubleshooting

This chapter covers potential problems and the corresponding remedies.

14.1 Problem Starting Up the ZyAIR

Table 14-1 Troubleshooting the Start-Up of Your ZyAIR

PROBLEM	CORRECTIVE ACTION	
None of the LEDs turn on when I plug in the power adapter.	Make sure you are using the supplied power adapter and that it is plugged in to an appropriate power source. Check that the power source is turned on. If the problem persists, you may have a hardware problem. In this case, you should contact your local vendor.	
I cannot access the ZyAIR via the console port.	1. Make sure the ZyAIR is connected to your computer's serial port.	
	2. Make sure the communications program is configured correctly. The communications software should be configured as follows:	VT100 terminal emulation.
		9600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed.
		No parity, 8 data bits, 1 stop bit, data flow set to none.

14.2 Problem with the Password

Table 14-2 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyAIR.	The **Password** and **Username** fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. Use the **RESET** button to restore the factory default configuration file. This will restore all of the factory defaults including the password. Refer to section on resetting to factory defaults for details.

14.3 Problem with the Ethernet Interface

Table 14-3 Troubleshooting the Ethernet Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyAIR from the Ethernet	If the all the LAN LEDs on the front panel are off, check the Ethernet cable connection between your ZyAIR and the computer connected to the LAN port. Check the faulty Ethernet cables. Make sure the NIC (Network Interface Card) on the Ethernet device is installed and working properly. Check the IP address of the Ethernet device. Make sure that the IP address and the subnet mask of the ZyAIR and the Ethernet device are on the same subnet.
I cannot ping any computer on the LAN.	Check the LAN LEDs on the front panel. One of these LEDs should be on. If they are all off, check the cables between your ZyAIR and the Ethernet device.

14.4 Problem with the WAN Interface

Table 14-4 Troubleshooting the WAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot get a WAN IP address from the ISP.	The WAN IP address is provided when the ISP recognizes the user as an authorized user after verifying the MAC address, Host Name or User ID. Find out the verification method used by your ISP. If the ISP checks the LAN MAC address, inform the ISP of the ZyAIR ‘s WAN MAC address. To view the WAN MAC address in SMT menu 24.1. In case the ISP does not allow you to use a new MAC, you can clone the MAC from the LAN as the WAN MAC and send it to the ISP using SMT menu 2. It is recommended that you configure this menu even if your ISP presently does not require MAC address authentication. If the ISP checks the Host Name, enter host name in the **System Name** field in the SMT menu 1 when you connect the ZyAIR to a cable/xDSL modem. If the ISP checks the User ID, make sure that you have entered the correct **Service Type**, user name (in the **My Login** field) and password (in the **My Password** field) in SMT menu 4.

14.5 Problem with Internet Access

Table 14-5 Troubleshooting the Internet Access

PROBLEM	CORRECTIVE ACTION
I cannot access the Internet.	Connect your cable/DSL modem with the ZyAIR using the appropriate cable. Check with the manufacturer of your cable/DSL device about your cable requirement because for some devices may require a crossover cable and others a straight-through Ethernet cable. Verify your WAN settings in SMT menu 2 and Internet access settings in SMT menu 4.
Internet connection disconnects	Check the schedule rules in SMT menu 26. If you use PPPoE encapsulation, check the idle time-out setting in SMT menu 11.5. Contact your ISP.

14.6 Problem with Telnet

Table 14-6 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyAIR through Telnet.	Refer to the *Problems with the Ethernet Interface* section for instructions on checking your Ethernet connection.

Appendix A
Wireless LAN and IEEE 802.11

A wireless LAN (WLAN) provides a flexible data communications system that you can use to access various services (navigating the Internet, email, printer services, etc.) without any expensive network cabling infrastructure. In effect a wireless LAN environment provides you the freedom to stay connected to the network while in the coverage area.

Benefits of a Wireless LAN

1. Access to network services in areas otherwise hard or expensive to wire, such as historical buildings, buildings with asbestos materials and classrooms.
2. Doctors and nurses can access a complete patient's profile on a handheld or notebook computer upon entering a patient's room.
3. It allows flexible workgroups a lower total cost of ownership for networks that are frequently reconfigured.
4. Conference room users can access the network as they move from meeting to meeting- accessing up-to-date information that facilitates the ability to communicate decisions "on the fly".
5. It provides campus-wide networking coverage, allowing enterprises the roaming capability to set up easy-to-use wireless networks that transparently covers an entire campus.

IEEE 802.11

The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize interoperability between differing brands of wireless LANs and to introduce a variety of performance improvements and benefits. On September 16, 1999, the 802.11b provided much higher data rates of up to 11Mbps, while maintaining the 802.11 protocol.

The IEEE 802.11 specifies three different transmission methods for the PHY, the layer responsible for transferring data between nodes. Two of the methods use spread spectrum RF signals, Direct Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS), in the 2.4 to 2.4825 GHz unlicensed ISM (Industrial, Scientific and Medical) band. The third method is infrared technology, using very high frequencies, just below visible light in the electromagnetic spectrum to carry data.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless nodes or stations (STA), which is called a Basic Service Set (BSS). In the most basic form, a

wireless LAN connects a set of computers with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). See the following diagram of an example of an Ad-hoc wireless LAN.

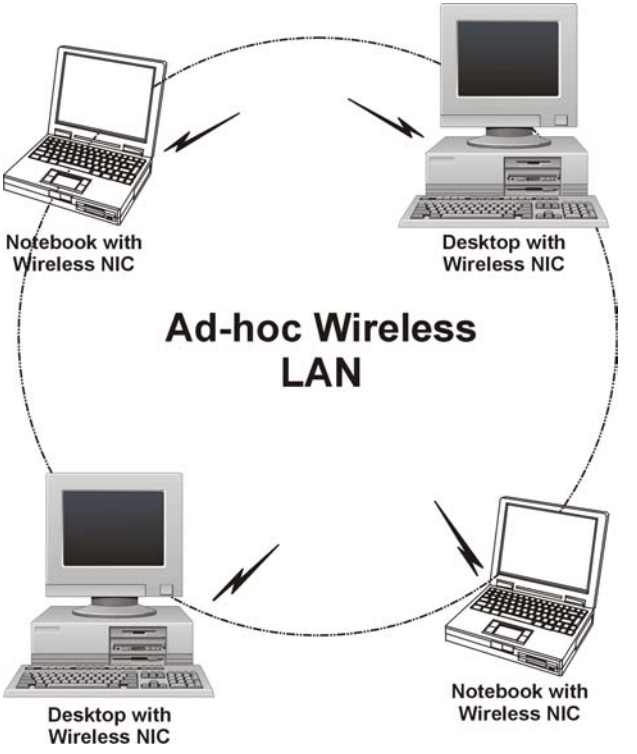

Diagram 1 Peer-to-Peer Communication in an Ad-hoc Network

Infrastructure Wireless LAN Configuration

For Infrastructure WLANs, multiple access points (APs) link the WLAN to the wired network and allow users to efficiently share network resources. The access points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple access points can provide wireless coverage for an entire building or campus. All communications between stations or between a station and a wired network client go through the access point.

The Extended Service Set (ESS) shown in the next figure consists of a series of overlapping BSSs (each containing an access point) connected together by means of a Distribution System (DS). Although the DS

could be any type of network, it is almost invariably an Ethernet LAN. Mobile nodes can roam between access points and seamless campus-wide coverage is possible.

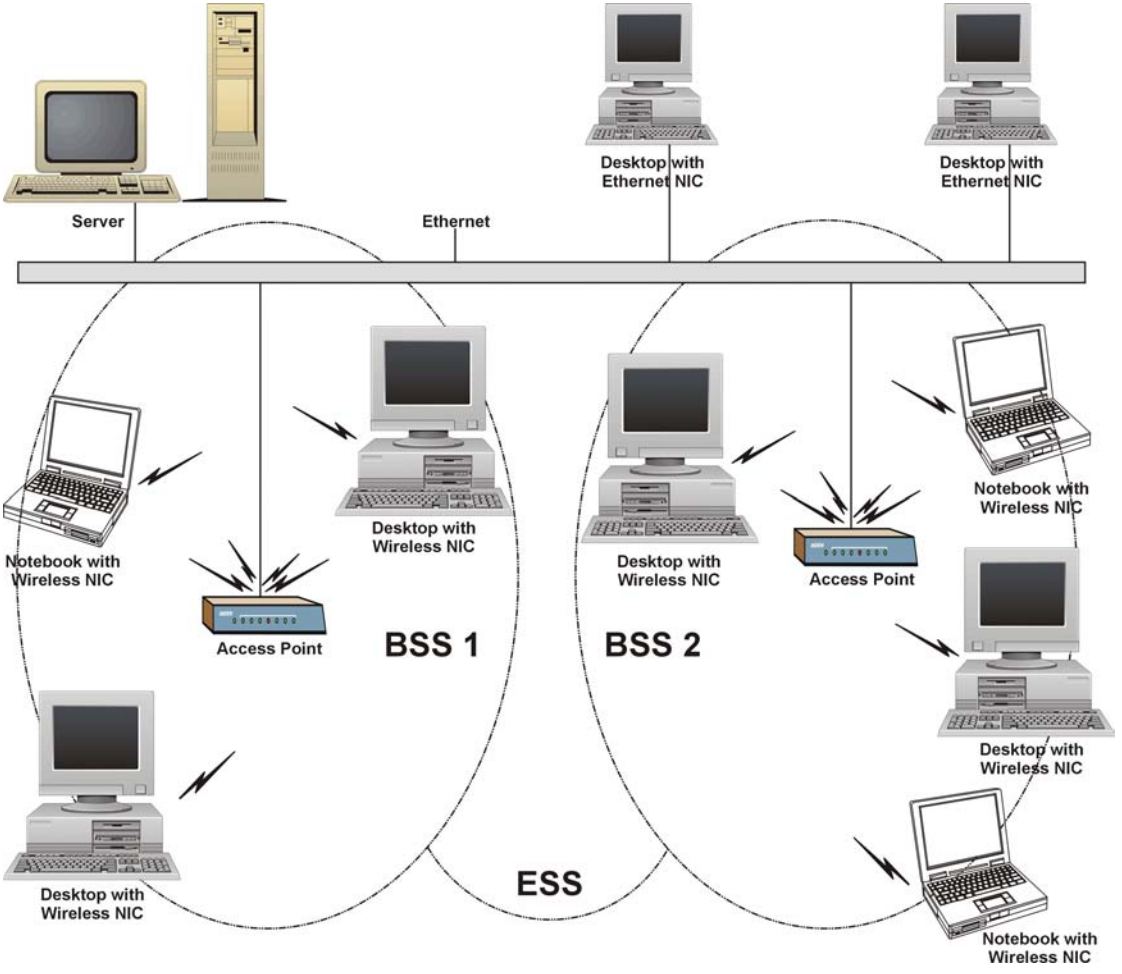

Diagram 2 ESS Provides Campus-Wide Coverage

Appendix B
Wireless LAN With IEEE802.1x

As wireless networks become popular for both portable computing and corporate networks, security is now a priority.

Security Flaws with IEEE 802.11

Wireless networks based on the original IEEE802.11 have a poor reputation for safety. The IEEE802.11b wireless access standard, first published in 1999, was based on the MAC address. As the MAC address is sent across the wireless link in clear text, it is easy to spoof and fake. Even the WEP (Wire Equivalent Privacy) data encryption is unreliable as it can be easily decrypted with current computer speed

Deployment Issues with IEEE 802.11

User account management has become a network administrator's nightmare in a corporate environment, as the IEEE 802.11b standard does not provide any central user account management. User access control is done through manual modification of the MAC address table on the access point. Although WEP data encryption offers a form of data security, you have to reset the WEP key on the clients each time you change your WEP key on the access point.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is already supported by Windows XP, other operating systems and a number of network devices.

Advantages of the IEEE 802.1x

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS Server Authentication Sequence

The following figure depicts a typical wireless network with a remote RADIUS server for user authentication using EAPOL (EAP Over LAN).

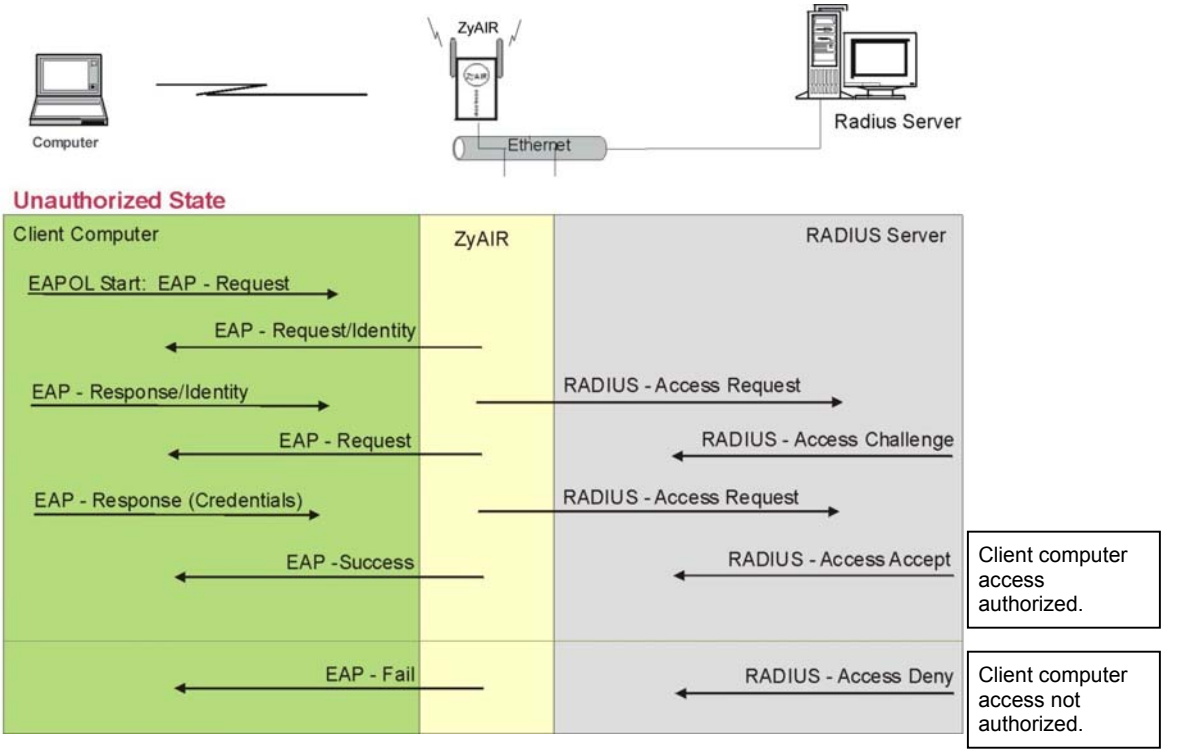

Diagram 3 Sequences for EAP MD5-Challenge Authentication

Appendix C
Antenna Selection and Positioning Recommendation

The access points in a wireless LAN send a radio frequency (RF) signal to the antennas, which propagate and capture the RF signal. Choosing the right antennas and positioning them properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

- **Frequency**

  An antenna in the frequency of 2.4GHz (IEEE 802.11b) or 5GHz(IEEE 802.11a) is needed to communicate efficiently in a wireless LAN.

- **Radiation Pattern**

  A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

- **Antenna Gain**

  Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

  For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

  Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas For WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight. The angle of the beam width determines the direction of the coverage pattern; typically ranges from 20 degrees (less

directional) to 90 degrees (very directional). The directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to – point application, position both transmitting and receiving antenna at the same height and in a direct line of sight to each other to attend the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

Appendix D
PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your PC to an ATM PVC (Permanent Virtual Circuit) which connects to an xDSL Access Concentrator where the PPP session terminates (see the next figure). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

Benefits of PPPoE

PPPoE offers the following benefits:

1. It provides you with a familiar dial-up networking (DUN) user interface.
2. It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN & ISDN), the switching fabric is already in place.
3. It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where PCs use traditional dial-up networking.

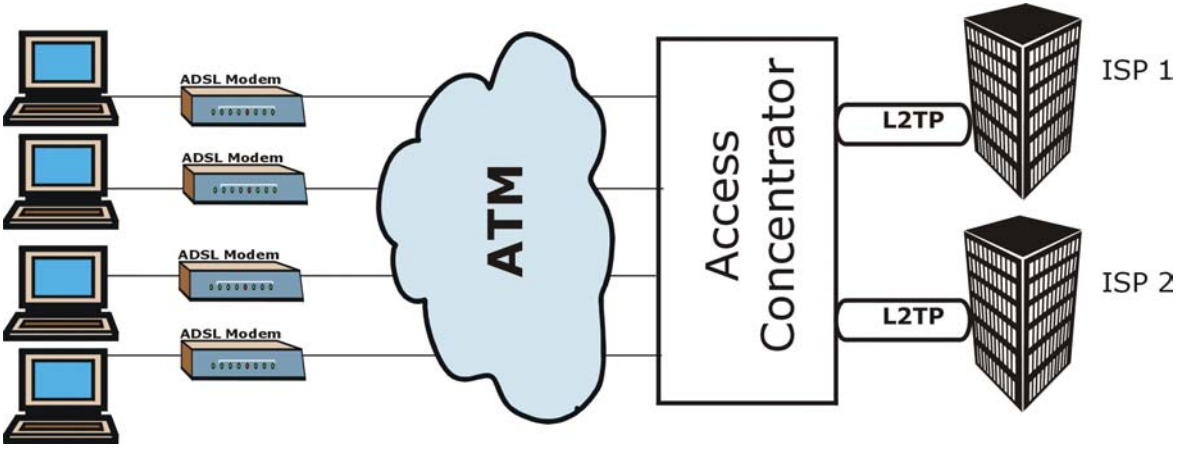

Diagram 4 Single-PC per Modem Hardware Configuration

How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the PC and the PC runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the PC and the ISP.

The ZyAIR as a PPPoE Client

When using the ZyAIR as a PPPoE client, the PCs on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual PCs.

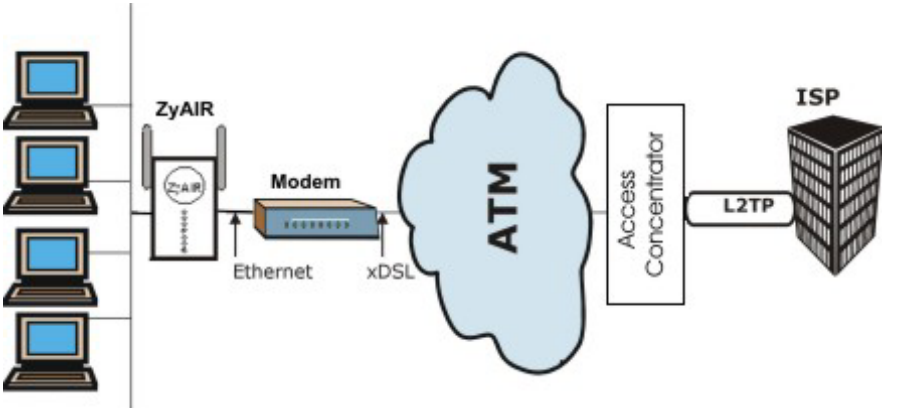

Diagram 5 ZyAIR as a PPPoE Client

Appendix E
PPTP

What is PPTP?

PPTP (Point-to-Point Tunneling Protocol) is a Microsoft proprietary protocol (RFC 2637 for PPTP is informational only) to tunnel PPP frames.

How can we transport PPP frames from a PC to a broadband modem over Ethernet?

A solution is to build PPTP into the ANT (ADSL Network Termination) where PPTP is used only over the short haul between the PC and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC 2364). The PPP connection, however, is still between the PC and the ISP. The various connections in this setup are depicted in the following diagram. The drawback of this solution is that it requires one separate ATM VC per destination.

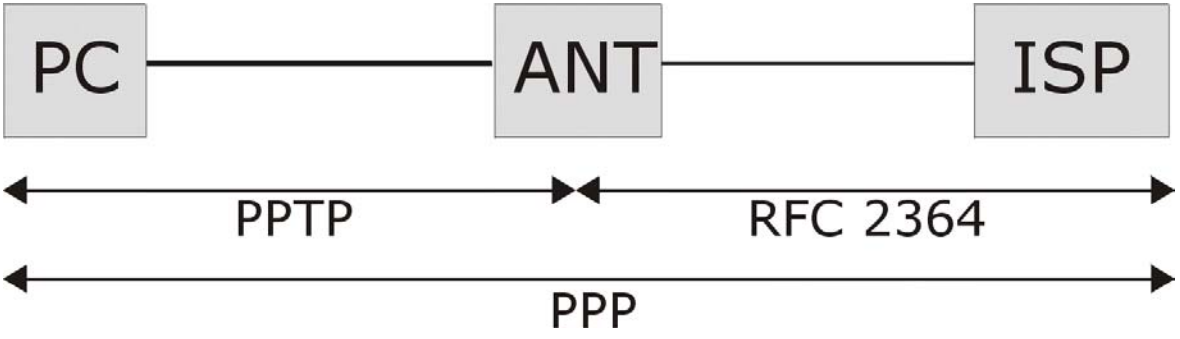

Diagram 6 Transport PPP frames over Ethernet

PPTP and the ZyAIR

When the ZyAIR is deployed in such a setup, it appears as a PC to the ANT (ADSL Network Termination).

In Windows VPN or PPTP Pass-Through feature, the PPTP tunneling is created from Windows 95, 98 and NT clients to an NT server in a remote location. The pass-through feature allows users on the network to access a different remote server using the ZyAIR's Internet connection. In NAT mode, the ZyAIR is able to pass the PPTP packets to the internal PPTP server (for example, NT server) behind the NAT. In the case above as the PPTP connection is initialized by the remote PPTP Client, the user must configure the PPTP clients. The ZyAIR initializes the PPTP connection, hence there is no need to configure the remote PPTP clients.

PPTP Protocol Overview

PPTP is very similar to L2TP, since L2TP is based on both PPTP and L2F (Cisco's Layer 2 Forwarding). Conceptually, there are three parties in PPTP, namely the PNS (PPTP Network Server), the PAC (PPTP Access Concentrator) and the PPTP user. The PNS is the box that hosts both the PPP and the PPTP stacks and forms one end of the PPTP tunnel. The PAC is the box that dials/answers the phone calls and relays the PPP frames to the PNS. The PPTP user is not necessarily a PPP client (can be a PPP server too). Both the PNS and the PAC must have IP connectivity; however, the PAC must in addition have dial-up capability. The phone call is between the user and the PAC and the PAC tunnels the PPP frames to the PNS. The PPTP user is unaware of the tunnel between the PAC and the PNS.

Diagram 7 PPTP Protocol Overview

Microsoft includes PPTP as a part of the Windows OS. In Microsoft's implementation, the PC, and hence the ZyAIR, is the PNS that requests the PAC (the ANT) to place an outgoing call over AAL5 to an RFC 2364 server.

Control and PPP Connections

Each PPTP session has distinct control connection and PPP data connection.

Call Connection

The control connection runs over TCP. Similar to L2TP, a tunnel control connection is first established before call control messages can be exchanged. Please note that a tunnel control connection supports multiple call sessions.

The following diagram depicts the message exchange of a successful call setup between a PC and an ANT.

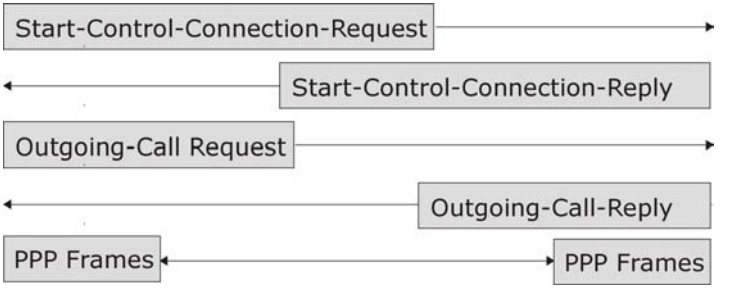

Diagram 8 Example Message Exchange between PC and an ANT

PPP Data Connection

The PPP frames are tunneled between the PNS and PAC over GRE (General Routing Encapsulation, RFC 1701, 1702). The individual calls within a tunnel are distinguished using the Call ID field in the GRE header.

Appendix F TCP/IP

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed. Use straight-through Ethernet cables to connect your computer's Ethernet adapter to a hub or switch and to connect the hub or switch to the ZyAIR's LAN port. Otherwise, connect your computer's Ethernet adapter directly to the LAN port with a crossover Ethernet cable.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

Setting up Your Windows 95/98/Me Computer

Installing TCP/IP Components

1. Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon.

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

a. In the **Network** window, click **Add**.

b. Select **Adapter** and then click **Add**.

c. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

a. In the **Network** window, click **Add**.

b. Select **Protocol** and then click **Add**.

c. Select **Microsoft** from the list of manufacturers.

d. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

a. Click **Add**.

b. Select **Client** and then click **Add**.

c. Select **Microsoft** from the list of manufacturers.

d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

e. Restart your computer so the changes you made take effect.

Configuring TCP/IP

1. In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**.
2. Click the **IP Address** tab.

   -If your IP address is dynamic, select **Obtain an IP address automatically**.

   -If you have a static IP address, select **Specify an IP address** and type your information into **the IP Address** and **Subnet Mask** fields.
3. Click the **DNS Configuration** tab.

   -If you do not know your DNS information, select **Disable DNS**.

   -If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).
4. Click the **Gateway** tab.

   -If you were not given a gateway IP address, remove previously installed gateways.

   -If you have a gateway IP address, type it in the **New gateway** field and click **Add**.
5. Click **OK** to save and close the **TCP/IP Pro**perties window.
6. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
7. Turn on your Prestige and restart your computer when prompted.

Verifying TCP/IP Properties

1. Click **Start** and then **Run**.
2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3. Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Setting up Your Windows NT/2000 Computer

Configuring TCP/IP

1. Click **Start**, **Settings**, **Network** and **Dial-up Connections** and right-click **Local Area Connection** or the connection you want to configure and click **Properties**.
2. Select **Internet Protocol (TCP/IP)** (you may need to scroll down) and click **Properties**.
3. The **Internet Protocol TCP/IP Properties** window opens.

   -If your IP address is dynamic, click **Obtain an IP address automatically**.

   -If you have a static IP address click Use the following IP Address and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
4. In the **Internet Protocol TCP/IP Properties** window:

   -Click **Obtain DNS server automatically** if you do not know your DNS server IP address(es).

   -If you know your DNS server IP address(es), type them in the **Preferred DNS server** and **Alternate DNS server** fields. If you have previously configured DNS servers, click **Advanced** and then the **DNS tab** to order them.
5. Click **Advanced**:

   -If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.
6. Click **OK** to save and close the **Internet Protocol (TCP/IP) Properties** window.
7. Click **OK** to close the **Local Area Connection Properties** window.
8. Turn on your Prestige and restart your computer (if prompted).

Verifying TCP/IP Properties

Click **Start**, **Programs**, **Accessories** and then **Command Prompt**.

In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. The window will display information about your connection-specific DNS suffix, IP Address, Subnet Mask and Default Gateway.

Setting up Your Windows XP Computer

Configuring TCP/IP

1. Click **start**, **Control Panel**, **Network and Internet Connections** and then **Network Connections**.
2. Right-click the network connection you want to configure and then click **Properties**.
3. Under the **General** tab, select Internet Protocol (TCP/IP) (you may need to scroll down) and click **Properties**.

4. The **Internet Protocol TCP/IP Properties** window opens.

   -If you have a dynamic IP address click **Obtain an IP address automatically**.

   -If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. To configure advanced static address settings for a local area connection, click **Advanced**, and do one or more of the following to configure additional IP addresses:

      -In the **IP Settings** tab, in **IP addresses**, click **Add**.

      -In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.

      -Repeat the above two steps for each IP address you want to add.

      -Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

      -In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.

      -Click **Add**.

      -Repeat the previous three steps for each default gateway you want to add.

      -Click **OK** when finished.

5. In the **Internet Protocol TCP/IP Properties** window's **General** tab:

   -Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).

   -If you know your DNS server IP address(es), click Use the following DNS server addresses, type them in the **Preferred DNS server** and **Alternate DNS server** fields. If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

6. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

7. Click **OK** to close the **Local Area Connection Properties** window.

8. Turn on your Prestige and restart your computer (if prompted).

Verifying TCP/IP Properties

1. Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support tab**.

Setting up Your Macintosh Computer

Configuring TCP/IP Properties

1. Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.
2. Select **Ethernet** from the **Connect via** list.
3. For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.
4. For statically assigned settings, do the following:

   -From the **Configure** box, select **Manually**.

   -Type your IP address in the **IP Address** box.

   -Type your subnet mask in the **Subnet mask** box.

   -Type the IP address of your Prestige in the **Router address** box.
5. Close the **TCP/IP Control Panel**.
6. Click **Save** if prompted, to save changes to your configuration.
7. Turn on your Prestige and restart your computer (if prompted).

Verifying TCP/IP Properties

Check your TCP/IP properties in the **TCP/IP Control Panel**.

Appendix G
IP Subnetting

IP Addressing

Routers "route" based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class "A" addresses have a 0 in the left most bit. In a class "A" address the first octet is the network number and the remaining three octets make up the host ID.
- Class "B" addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class "B" address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class "C" addresses begin (starting from the left) with 1 1 0. In a class "C" address the first three octets make up the network number and the last octet is the host ID.
- Class "D" addresses begin with 1 1 1 0. Class "D" addresses are used for multicasting. (There is also a class "E" address. It is reserved for future use.)

Chart 1 Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

Host IDs of all zeros or all ones are not allowed.

Therefore:

- A class "C" network (8 host bits) can have 2^8 –2 or 254 hosts.
- A class "B" address (16 host bits) can have 2^{16} –2 or 65534 hosts.

A class "A" address (24 host bits) can have 2^{24} –2 hosts (approximately 16 million hosts).

Since the first octet of a class “A” IP address must contain a “0”, the first octet of a class “A” address can have a value of 0 to 127.

Similarly the first octet of a class “B” must begin with “10”, therefore the first octet of a class “B” address has a valid range of 128 to 191. The first octet of a class “C” address begins with “110”, and therefore has a range of 192 to 223.

Chart 2 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191
Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	224 to 239

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 bits; each bit of the mask corresponds to a bit of the IP address. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The “natural” masks for class A, B and C IP addresses are as follows.

Chart 3 “Natural” Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class "C" address using both notations.

Chart 4 Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

The first mask shown is the class "C" natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class "C" address 192.168.1.0 with subnet mask of 255.255.255.0.

	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class "C"). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The "borrowed" host ID bit can be either "0" or "1" thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

In the following charts, shaded/bolded last octet bit values indicate host ID bits "borrowed" to form network ID bits. The number of "borrowed" host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after "borrowing") determines the number of hosts you can have on each subnet.

Chart 5 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**0**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Chart 6 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**1**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is $2^7 - 2$ or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

Chart 7 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Chart 8 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Chart 9 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Chart 10 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

More Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110) and so on.

The following table is a summary for class "C" subnet planning.

Chart 11 Class C Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Subnetting With Class A and Class B Networks.

For class "A" and class "B" addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class "B" address has two host ID octets available for subnetting and a class "A" address has three host ID octets (see *Chart 1*) available for subnetting.

The following table is a summary for class "B" subnet planning.

Chart 12 Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Appendix H
Power Adapter Specifications

NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	**AD48-1201200DUY**
Input Power	AC120Volts/60Hz/0.25A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	UL, CUL (UL 1950, CSA C22.2 No.234-M90)
NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	**DV-121A2-5720**
Input Power	AC120Volts/60Hz/27VA
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223-M91)
EUROPEAN PLUG STANDARDS	
AC Power Adapter Model	**AD-1201200DV**
Input Power	AC230Volts/50Hz/0.2A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	TUV, CE (EN 60950)
UNITED KINGDOM PLUG STANDARDS	
AC Power Adapter Model	**AD-1201200DK**
Input Power	AC230Volts/50Hz/0.2A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	TUV, CE (EN 60950, BS7002)

JAPAN PLUG STANDARDS	
AC Power Adapter Model	**JOD-48-1124**
Input Power	AC100Volts/ 50/60Hz/ 27VA
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	T-Mark (Japan Dentori)
AUSTRALIA AND NEW ZEALAND PLUG STANDARDS	
AC Power Adapter Model	**AD-1201200DS** or **AD-121200DS**
Input Power	AC240Volts/50Hz/0.2A
Output Power	DC12Volts/1.2A
Power Consumption	10 W
Safety Standards	NATA (AS 3260)

Index

4

4-Port Switch 1-1

A

Ad-hoc Configuration ..... A
Antenna 2-4
  Directional ..... G
  Omni-directional ..... G
  Types ..... G
Antenna gain ..... G
AT command 10-1
Authentication 5-3, 5-4
auto-negotiation 1-1

B

Back Panel
  connections description 2-3
Backup 10-2
Basic Service Set ..... A
Benefits of PPPoE I
BSS ..... See Basic Service Set

C

Call Connection L
Call Filtering 7-1
Call Filters
  Built-In 7-1
  User-Defined 7-1
Call Scheduling 12-1
  Maximum Number of Schedule Sets 12-1
  PPPoE 12-3
  Precedence 12-1
  Precedence Example ..... See precedence
CDR 9-6
CDR (Call Detail Record) 9-5
Channel ID 3-16
CHAP 5-3
Clear to Send protocol 3-14
Collision 9-2
Command Interpreter 11-1
Community 8-2
Computer Name 2-12
Conditions that prevent TFTP and FTP from
  working over WAN 10-4
Connecting to a Cable Modem 2-3
Connecting to a DSL Modem 2-3
Connections
  Additional Requirements 2-5
  ADSL Line 2-3
  Console Port 2-4
  Power Adapter 2-4
  Rear Panel 2-3
Control and PPP Connections L
Copyright ii
Cost Of Transmission 5-6, 5-9
Coverage 2-5
CPU Load 9-2
Crossover Ethernet Cable 2-3
CTS ..... See Clear to Send
Customer Support v

D

data collision 3-14
Data Filtering 7-1
Device Filter rules 7-12
DHCP 1-3, 9-4
Diagnostic 9-7
Diagnostic Tools 9-1
Direct Sequence Spread Spectrum ..... A
Distribution System ..... B
DNS 3-6
Domain Name 6-13
Domain Name System 3-4
DS ..... See Distribution System
DSSS ..... See Direct Sequence Spread Spectrum
Dynamic DNS 1-2, 2-13, 2-14

Dynamic Host Configuration Protocol 3-4
Dynamic Service Selection 3-10
DYNDNS Wildcard 2-13

E

EAP 4-3
EAP Authentication Sequence 4-4
Encapsulation 3-10, 3-12, 5-1
Error Log 9-5
Error/Information Messages
  Sample 9-5
ESS ..... See Extended Service Set
ESS ID 3-14
Ethernet 3-10
Ethernet Encapsulation 6-12
Ethernet Traffic 7-16
Extended Service Set ..... B
External Hub 2-3

F

FCC iii
FHSS ... See Frequency-Hopping Spread Spectrum
Filename Conventions 10-1
Filter 2-17
  Applying Filters 7-15
  Ethernet traffic 7-16
  Ethernet Traffic 7-16
  Filter Rules 7-5
  Filter Structure 7-3
  Generic Filter Rule 7-11
  Remote Node 5-6
  Remote Node Filter 5-6
  Remote Node Filters 7-16
  Sample 7-14
  SUA 7-12
  TCP/IP Filter Rule 7-6
Filter Log 9-6
Filter Rule 7-7
Filter Rule Process 7-2
Filter Rule Setup 7-6
Filter Rules Summary
  Sample 7-15
Filter Set
  Class 7-6
Filter Set Configuration 7-3
Filtering 7-1, 7-6
Fragment Threshold 3-16
Fragmentation Threshold 3-15
Frequency-Hopping Spread Spectrum ..... A
FTP 13-3
  Restrictions 13-3
FTP File Transfer 10-10
FTP Restrictions 10-4
FTP Server 6-19

G

Gateway 5-9
General Setup 2-12

H

Hidden Menus 2-10
Hidden Node problem 3-14
Hop Count 5-6, 5-9
How PPPoE Works ..... J
HTTP 6-13
HyperTerminal program 10-6, 10-9

I

IANA 3-2, 3-3
IBSS ..... See Independent Basic Service Set
IEEE 802.11 ..... A
  Deployment Issues ..... E
  Security Flaws ..... E
IEEE 802.11b 1-1
IEEE 802.1x 1-2
  Advantages ..... E
IGMP support 5-6
Independent Basic Service Set ..... B
Infrastructure Configuration ..... B
Initialization 2-7
Internet access 3-1
Internet Access 1-2, 1-4, 2-11, 3-1, 3-11, 3-12

Internet Access Setup 6-6
Internet Assigned Numbers Authority ..See IANA
IP Address 3-7, 5-9, 7-8, 9-4, 9-7
IP Address Assignment 3-11
IP Alias Setup 3-8
IP Filter 7-10
  Logic Flow 7-9
IP mask 7-8
IP Multicast 1-3
IP network number 3-2
IP Packet 7-11
IP Pool 3-4
IP Static Route 5-7
IP Static Route Setup 5-8

L

Link type 9-2
Log and Trace 9-5
Log Facility 9-6
Logging Option 7-9, 7-12

M

MAC Address
  Cloning Recommendation 2-15
MAC Address Filter Action 4-10
MAC Address Filtering 4-8
Main Menu 2-10
Management Information Base (MIB) 8-2
Message Logging 9-4
Metric 5-6, 5-9
Mounting Options 2-5
Multicast 5-6
My WAN Address 5-5

N

Nailed-Up Connection 5-1
NAT 7-12
  Application 6-3
  Applying NAT in the SMT Menus 6-6
  Configuring 6-7
  Definitions 6-1
  Examples 6-16
  How NAT Works 6-2
  Mapping Types 6-4
  Non NAT Friendly Application Programs 6-21
  Ordering Rules 6-12
  What NAT does 6-2
Network Address Translation 3-13
Network Address Translation (NAT) 6-1
Network Management 1-3
Network Topology With RADIUS Server
  Example ..... E

P

Packet Triggered 9-6
Packets 9-2
PAP 5-3
Password 2-7, 2-12, 5-3, 8-2
Ping 9-7
PPP Data Connection ..... M
PPP Log 9-6
PPPoE I
PPPoE Encapsulation 3-10
PPPoE in Action I
PPTP ..... K
PPTP Encapsulation 3-10
PPTP Protocol Overview L
PPTP Support 1-2
Private 5-6, 5-9
Protocol 7-7
Protocol Filter Rules 7-12

Q

Quick Start Guide xvii

R

RADIUS 4-3
  Shared Secret Key 4-4
RADIUS Message Types 4-3
RAS 9-4
Rate
  Receiving 9-2

Transmission 9-2
Related Documentation.....xvii
Remote Authentication Dial In User Service... See RADIUS
Remote DHCP Server..... 3-7
Remote Management Limitations..... 13-3
Remote Management Setup 13-1, 13-2
Remote Node 5-1, 9-2
Remote Node Profile 5-2
Request to Send protocol 3-14
Required fields..... 2-10
RESET Button 2-4
Restore Configuration..... 10-7
Reverse SMA connectors..... 2-4
RF signals .....A
RIP .... 3-7, 5-6. See Routing Information Protocol
Roaming..... 3-16
Enable on ZyAIR..... 3-18
Example..... 3-17
Requirements..... 3-17
Routing Information Protocol..... 3-3
Direction..... 3-3
Version 3-3
RTS..... See Request to Send
RTS Threshold..... 3-14, 3-16

S

Schedule Sets
Duration..... 12-2
Server..6-5, 6-7, 6-9, 6-11, 6-12, 6-13, 6-14, 6-17, 6-18
Service iv
setup a schedule 12-2
Single-PC per Modem Hardware Configuration . I
SMT Menu Overview 2-8
SNMP
Community..... 8-3
Configuration..... 8-2
Get 8-2
Manager..... 8-2
MIBs..... 8-2
Trap 8-2
Traps 8-3
Trusted Host.....8-3
Static Route Setup 5-7
Static Routing Topology.....5-8
STP 2-3
SUA (Single User Account) ..... See NAT
Subnet Mask 3-2, 3-7, 5-5, 5-9, 9-4
Support Disk.....xvii
Supporting Disk.....xvii
Syntax Conventions.....xviii
Syslog 9-5
Syslog IP Address 9-6
Syslog Server.....9-5
System
Console Port Speed 9-4
Diagnostic 9-7
Log and Trace 9-4
Syslog and Accounting 9-5
System Information.....9-3
System Status 9-1
Time and Date.....11-2
System Information 9-3
System Information & Diagnosis 9-1
System Maintenance...9-1, 9-3, 10-2, 10-5, 10-13, 10-14, 11-1, 11-2
System Management Terminal.....2-10
System Timeout.....13-4

T

TCP/IP 7-12, 9-7, 13-1
TCP/IP Parameters 3-2
Telnet.....13-1
Telnet Configuration 13-1
Telnet Under NAT.....13-1
TFTP
And FTP Over WAN}.....13-3
Restrictions.....13-3
TFTP and FTP over WAN Will Not Work
When….....10-4
TFTP File Transfer 10-12

TFTP Restrictions 10-4
The Teledat Router as a PPPoE Client ..... J
Time and Date Setting 11-2
Time Server 11-2
Time Zone 11-3
To avoid damage to the ZyAIR 2-4
Trace Records 9-4
Traditional Dial-up Scenario I
Troubleshooting
  Accessing ZyAIR B-1000 14-3
  Ethernet Port 14-2
  Password 14-1
  Start-Up 14-1

U

UNIX Syslog 9-4, 9-6
UNIX syslog parameters 9-6
Upload Firmware 10-10
User Profiles 4-7

V

Valid CI Commands 11-1

W

WEP 3-15
WEP Encryption 4-2
What is PPTP? ..... K
Wired Equivalent Privacy ..... See WEP. See WEP
Wireless LAN ..... A, 3-13
  Benefits ..... A
Wireless LAN Setup 3-15
WLAN ..... See Wireless LAN

X

XMODEM protocol 10-2

Z

ZyNOS 10-1, 10-2
ZyNOS F/W Version 10-1
ZyXEL Limited Warranty
  Note iv
Error! Not a valid document self-reference on page 18